# ccbpm数据安全保障

# 概述

* 数据安全软件开发系统的永恒话题，驰骋按照自己方式来解决数据安全。
* 数据安全多个方面：我们从登录用户安全、数据传输加密、SQL加密、实体操作安全几个方面来应对日益重要的数据安全。
* 驰骋交付的客户都满足等保需求，经过压力测试，安全测试认证。

# 用户名密码

* 密码的存储配置模式分为：

1. 明文密码
2. MD5加密密码
3. BCrypt加密密码

* 密码的组合配置模式分为：

1. 无要求
2. 8-20位字符,必须包含大小写字母、数字并且不得包含用户名

* 密码强制修改的配置

1. 第一次登录时，是否强制修改默认密码

* 密码传输时的安全

1)登录、密码修改等涉及密码传输的地方，均需要通过AES加密后传输.

# Token模式

* 后端Token的存储

1. 单服务环境，内存存储
2. 集群服务环境,redis存储

* 前端存储

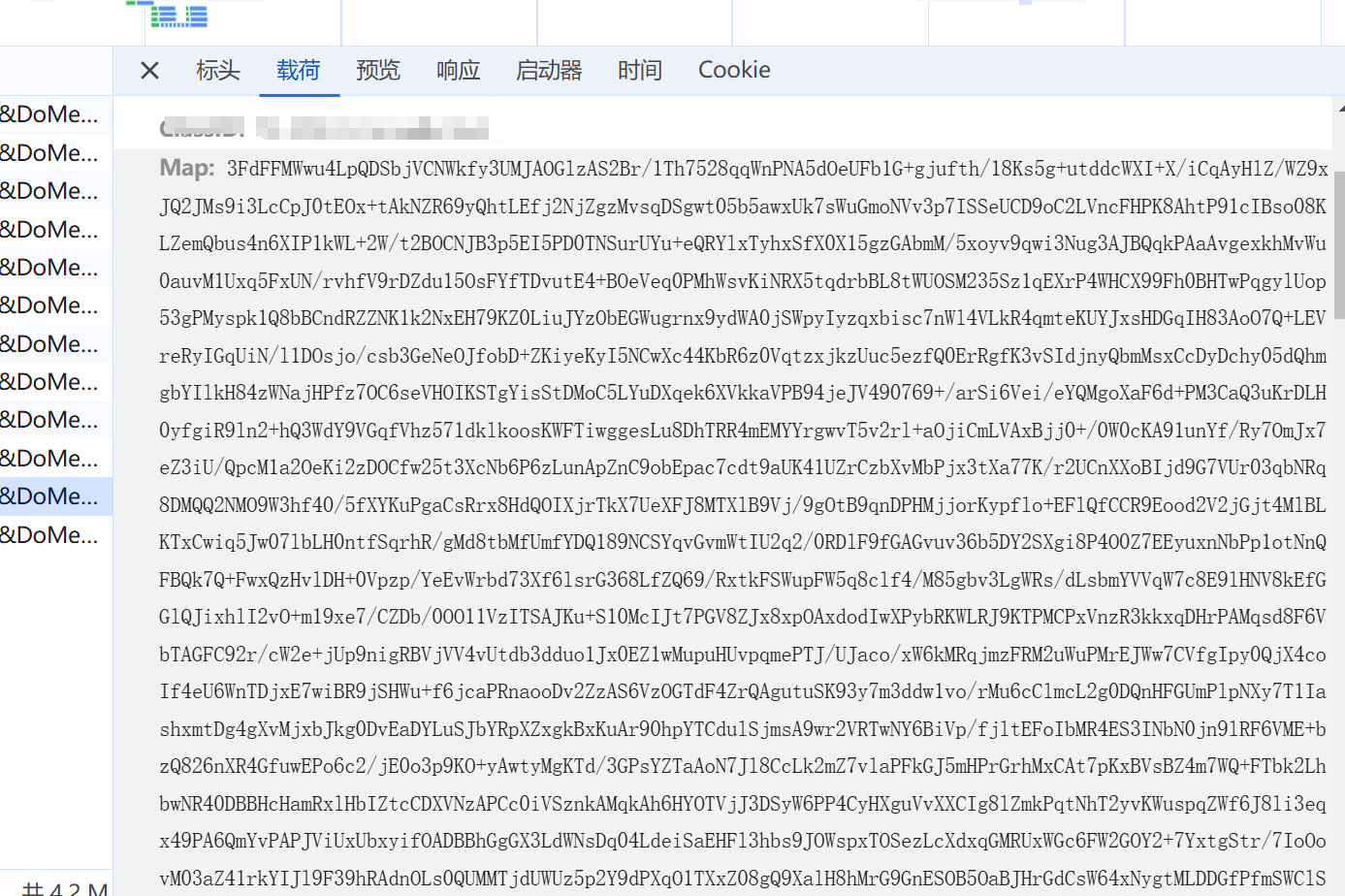
使用ts泛型创建接口和实现类，用于更安全地管理localStorage和sessionStorage中的数据

* Token的工作模式
  + 永久有效
  + 单设备登录
* Token过期设置

定期刷新或撤销token

# 数据传输加密

* 前后端的数据传输是按照加密的方式处理的。
* 对于敏感的数据，如前端实体的核心定义和在用户界面中动态配置的SQL，都通过加密传输，即使不使用SSL证书，也能保证数据传输过程中难以被解密。



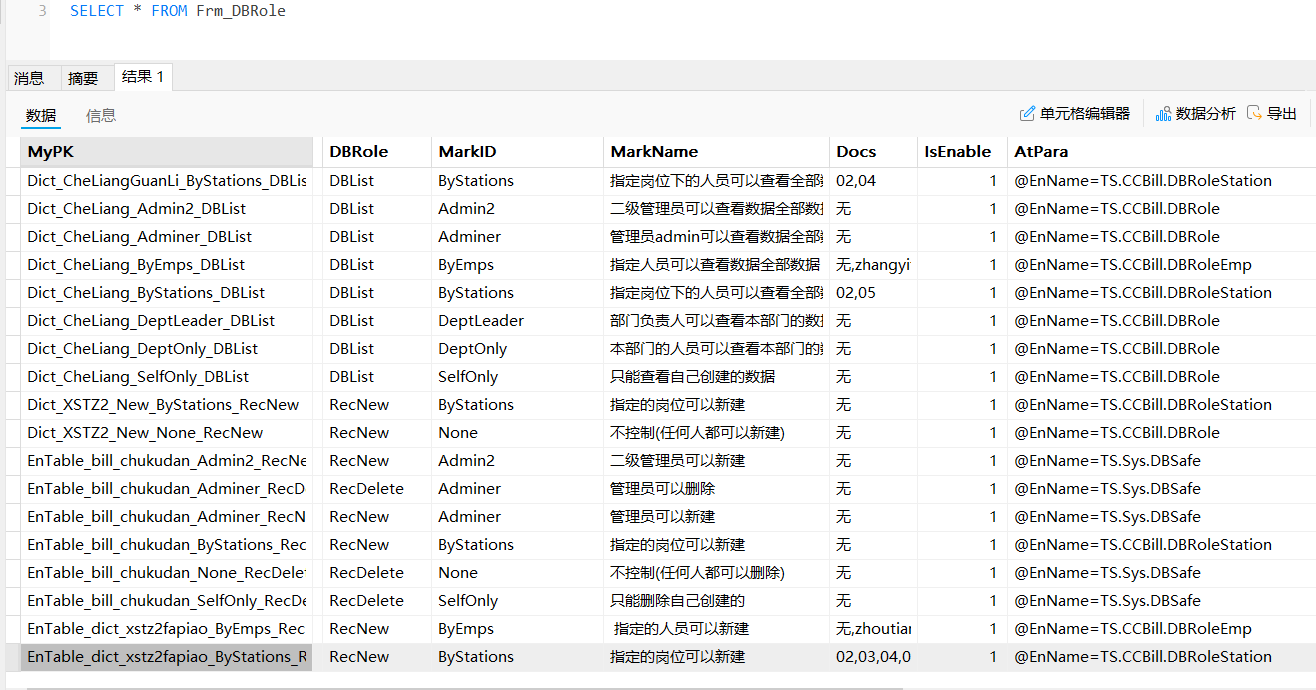


* 加密算法使用常见的AES-CBC

# 配置SQL执行

* 表单设计器中的字段的扩展属性配置的SQL语句在后端执行。
* 模糊查询如何的值前端进行了过滤，禁止输入;\*--\' "
* 防止调用接口中传参含有特殊字符，在后端中参数进行过滤，过滤掉参数中的;\*--\' "

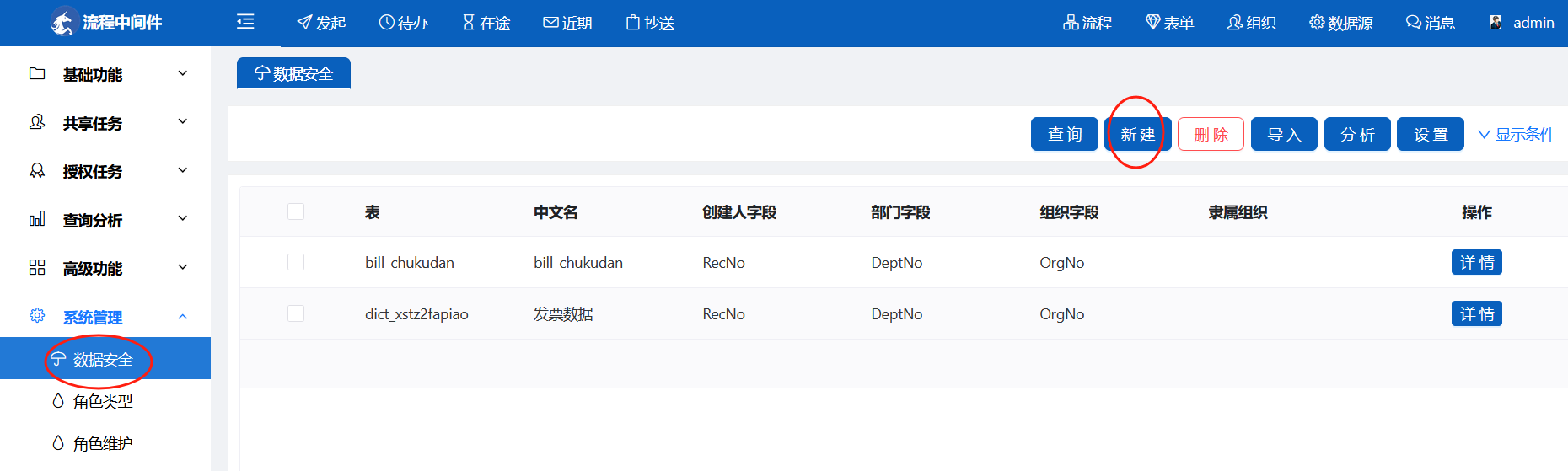
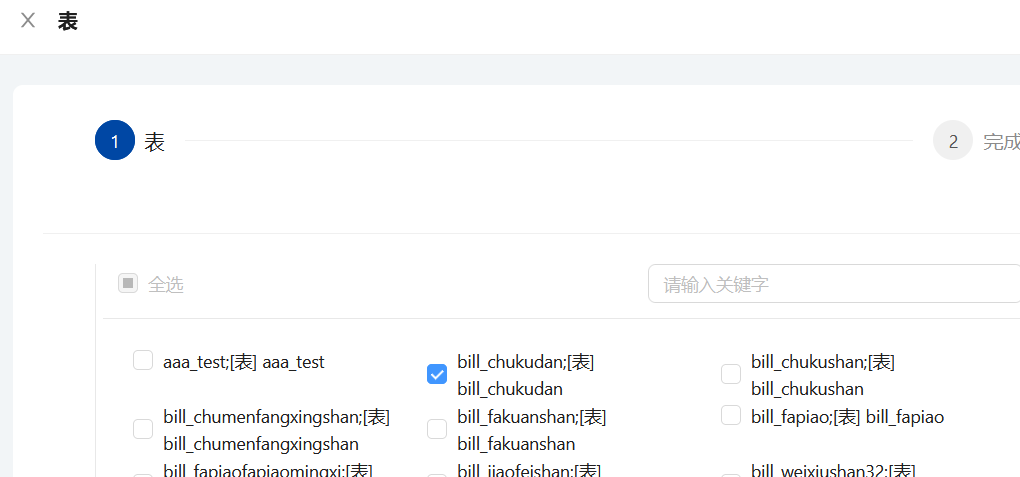
# 实体单据的安全(前端)

* 实体对应的是数据库，ccfast是按照数据表来进行控制权限的。
* 数据权限的存储在Frm\_DBRole表里，如下图：
* 

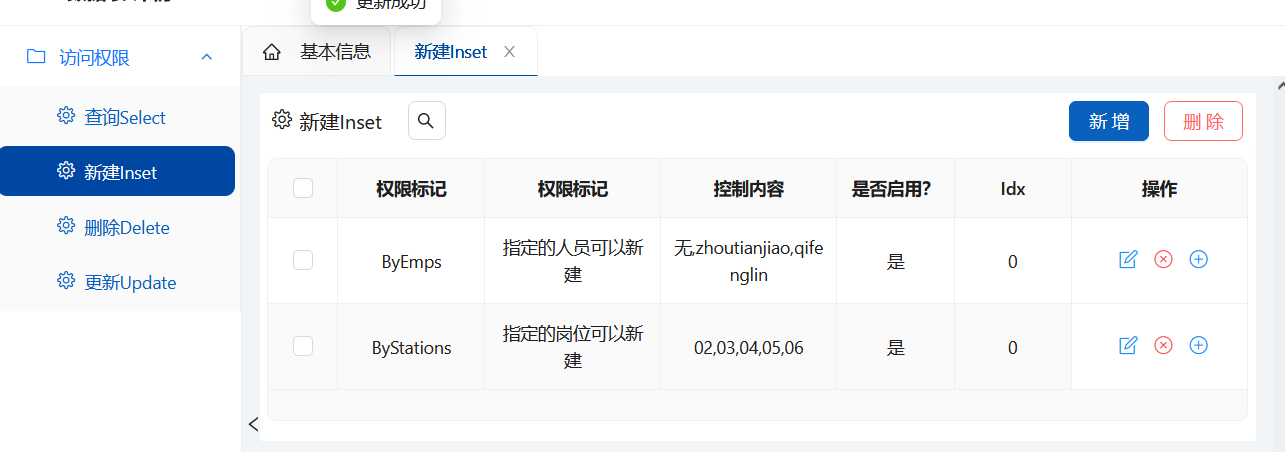
## 管理员权限

* 按照应用来分：业务逻辑定义实体类，业务逻辑类，管理员操作的类库都是在指定的命名空间里。
* 系统对管理员操作的类库不再区分权限。
* 比如：TS.Sys,TS.Port 相关系的类不控制权限。
* 默认对指定的实体是不进行权限控制的，如果需要权限控制，就需要对他进行设定。

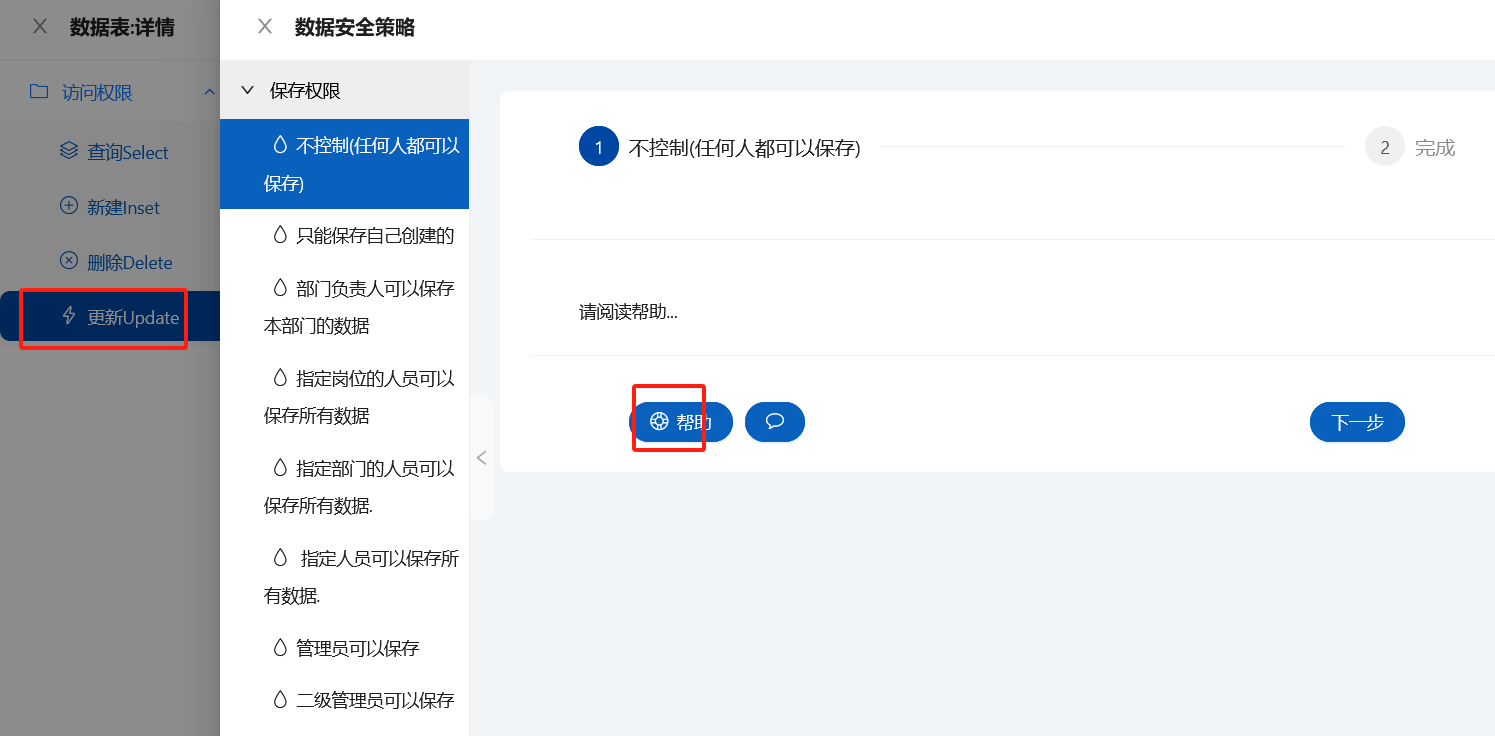
## 对指定的表权限管理

1. 选择要控制的表，一个表可以对应多个前端实体类。
2. 
3. 加入控制策略库，按照insert,delete,update, select 三个类型分配控制权限。
4. 

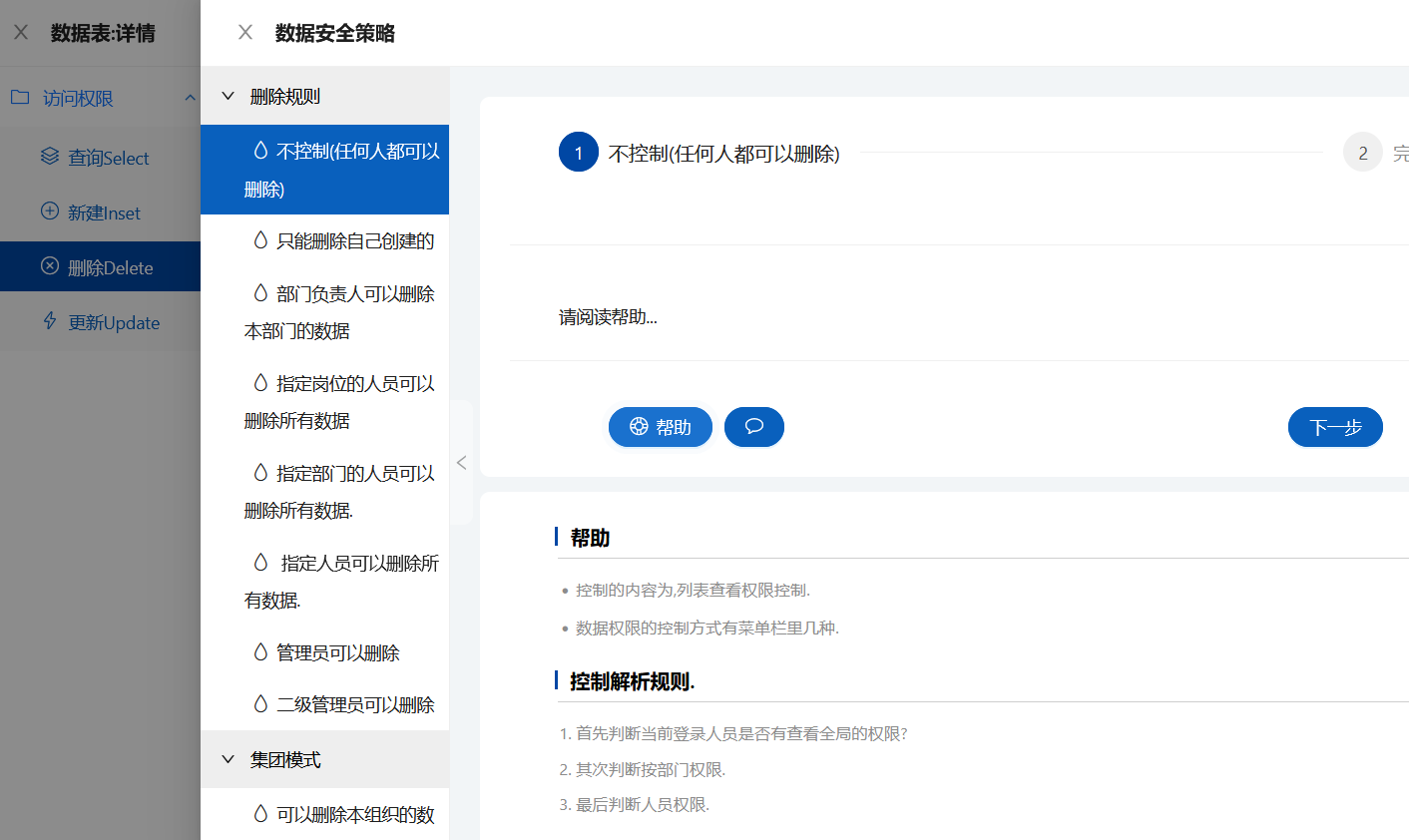
## 插入权限

* 对数据执行insert的权限。
* 
* 控制方式：
* 

## 修改权限

1. 对数据执行update的权限。
2. 

## 删除权限

1. 删除权限.
2. 

## 查询权限

1. 查询权限控制.
2. 

# 解决事务问题

* 处理不同数据库的事务。
* 未编写。

# 附件上传

* 支持多种模式，每个模式都有自己的安全保护措施。
* 存储数据库模式：由数据库管理员保障数据安全。
* 存储到OSS：由OSS提供商保护安全，ccbpm通过用户名密码调用。
* 禁止上传.msi, .bat, .js, .ts的危险可执行的文件。

===OVER===