权限管理模块

[权限管理模块 1](#_Toc467768570)

[1 主要接口 1](#_Toc467768571)

[1.1登录 1](#_Toc467768572)

[1.2登出 2](#_Toc467768573)

[1.3授权 根据token获取权限信息 2](#_Toc467768574)

[2 权限控制主要实体及关系 2](#_Toc467768575)

[2.1主要实体定义 2](#_Toc467768576)

[2.1.1用户信息表 T\_USER 2](#_Toc467768577)

[2.1.2角色信息表 T\_ROLE 3](#_Toc467768578)

[2.1.3权限信息表 T\_PERMISSION 3](#_Toc467768579)

[2.1.4用户角色关系表 R\_USER\_ROLE 3](#_Toc467768580)

[2.1.5角色权限关系表 R\_ROLE\_PERMISSION 4](#_Toc467768581)

[2.2实体关系图 5](#_Toc467768582)

[3权限控制规则 5](#_Toc467768583)

[3.1接口层级控制 5](#_Toc467768584)

[3.1.1利用角色控制访问 6](#_Toc467768585)

[3.1.2利用预定义权限控制访问 6](#_Toc467768586)

[3.2代码级别控制 6](#_Toc467768587)

# 1 主要接口

## 1.1登录

POST http://{host}:{port}/authc/api/{v1}/tokens

入参：

{

“username”:”{username}”,

“password”:”{password}”

}

返回值:

200

{

“token”:”{token}”,

“userId”:”{userId}” //用户OID

}

## 1.2登出

DELETE http://{host}:{port}/authc/api/{v1}/tokens/{tokenid}

返回值：

204 No Content

## 1.3授权 根据token获取权限信息

GET http://{host}:{port}/authc/api/{v1}/authorizations/{tokenid}?ip={terminalIpAddress}

返回值：

200

{

“id”:””,

“username”:””,

“roles”:”[]”,

“permissions”:”[]”

}

备注：返回值属性需要根据后续的业务需要来更新

# 2 权限控制主要实体及关系

## 2.1主要实体定义

### 2.1.1用户信息表 T\_USER

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **列名** | **数据类型** | **约束** | **默认值** | **备注** |
| ID | Bigint | PK |  |  |
| CODE |  |  |  | 员工编号 |
| USERNAME |  | M |  | 登录用户名 |
| PASSWORD |  | M |  |  |
| NAME |  | M |  | 姓名 |
| GENDER | Char(1) |  |  |  |
| MOBILE\_PHONE |  |  |  |  |
| TELEPHONE |  |  |  |  |
| EMAIL |  |  |  |  |
| IS\_ACTIVE | Char(1) |  | Y |  |
| IS\_LOCKED | Char(1) |  | N |  |
| IS\_DELETED | Char(1) |  | N |  |
| CREATE\_AT |  |  |  |  |
| UPDATE\_AT |  |  |  |  |
| CREATE\_BY |  |  |  |  |
| UPDATE\_BY |  |  |  |  |
| DATA\_SOURCE | Varchar(30) |  |  | SYSTEM HIS |

### 2.1.2角色信息表 T\_ROLE

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **列名** | **数据类型** | **约束** | **默认值** | **备注** |
| ID | Bigint | PK |  |  |
| CODE |  |  |  | 角色编码 |
| NAME |  | M |  | 角色名称 |
| LABEL |  |  |  | 用来前端默认显示 |
| DESCRIPTION |  |  |  |  |
| IS\_DELETED | Char(1) |  | N |  |
| CREATE\_AT |  |  |  |  |
| UPDATE\_AT |  |  |  |  |
| CREATE\_BY |  |  |  |  |
| UPDATE\_BY |  |  |  |  |
| DATA\_SOURCE | Varchar(30) |  |  | STATIC,SYSTEM, HIS |

### 2.1.3权限信息表 T\_PERMISSION

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **列名** | **数据类型** | **约束** | **默认值** | **备注** |
| ID | Bigint | PK |  |  |
| CODE |  |  |  | 权限编码 |
| NAME |  | M |  | 权限名称 |
| LABEL |  |  |  | 用来前端默认显示 |
| DESCRIPTION |  |  |  |  |
| IS\_DELETED | Char(1) |  | N |  |

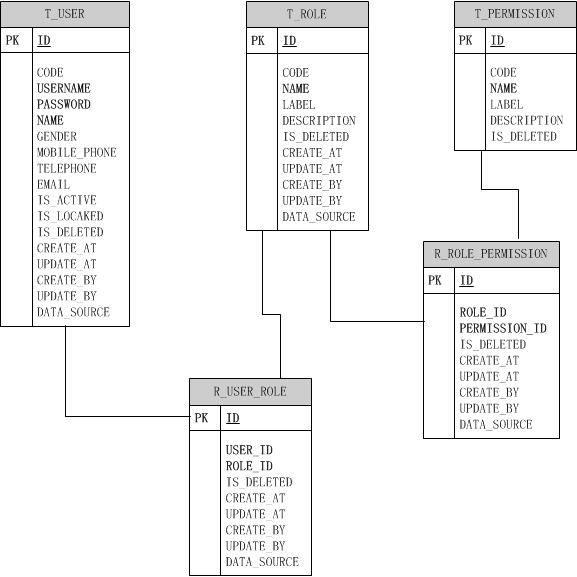
### 2.1.4用户角色关系表 R\_USER\_ROLE

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **列名** | **数据类型** | **约束** | **默认值** | **备注** |
| ID | Bigint | PK |  |  |
| USER\_ID |  | M, FK |  |  |
| ROLE\_ID |  | M, FK |  |  |
| IS\_DELETED | Char(1) |  | N |  |
| CREATE\_AT |  |  |  |  |
| UPDATE\_AT |  |  |  |  |
| CREATE\_BY |  |  |  |  |
| UPDATE\_BY |  |  |  |  |
| DATA\_SOURCE |  |  |  |  |

### 2.1.5角色权限关系表 R\_ROLE\_PERMISSION

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **列名** | **数据类型** | **约束** | **默认值** | **备注** |
| ID | Bigint | PK |  |  |
| ROLE\_ID |  | M, FK |  |  |
| PERMISSION\_ID |  | M, FK |  |  |
| IS\_DELETED | Char(1) |  | N |  |
| CREATE\_AT |  |  |  |  |
| UPDATE\_AT |  |  |  |  |
| CREATE\_BY |  |  |  |  |
| UPDATE\_BY |  |  |  |  |
| DATA\_SOURCE |  |  |  |  |

## 2.2实体关系图





# 3权限控制规则

## 3.1接口层级控制

/non-login-urls/\*\*=anon

/nurses/\*\*=authcToken,roles[NURSE,HEAD\_NURSE],perms[SYSTEM:LOGIN]

/\*\*=authcToken,perms[SYSTEM:LOGIN]

### 3.1.1利用角色控制访问

roles[NURSE,HEAD\_NURSE]

### 3.1.2利用预定义权限控制访问

perms[SYSTEM:LOGIN]

## 3.2代码级别控制

通过元注释控制代码方法的访问权限，示例如下：

@RequiresPermissions("DEPT:LIST")

@RequiresRoles("HEAD-NURSE")