**IAM AD系统模块**

**详细设计书**

**IAM Project Team**

**2014年10月**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号  No | 修改人  Change Person | 修改日期  Change Date | 基准时间  Base Line Time | 修改内容  Detail |
| 1 | Xu haibo | 2014-10-30 |  | Create |
| 2 | Xu haibo | 2014-10-31 |  | Edit |
| 3 | Xu haibo | 2014-11-1 |  | Edit |
|  |  |  |  |  |

目录

[1、文档概述 4](#_Toc403085543)

[1.1、范围 4](#_Toc403085544)

[1.2相关文档 4](#_Toc403085545)

[2、E-HR系统软件设计 5](#_Toc403085546)

[2.1员工类账号 5](#_Toc403085547)

[2.2、其他类型账号 7](#_Toc403085548)

[2.3、系统类账号 10](#_Toc403085549)

[3、HEC系统软件设计 13](#_Toc403085550)

[3.1、员工类账号 13](#_Toc403085551)

[3、 TC软件系统设计 14](#_Toc403085552)

[4.1、员工类账号 15](#_Toc403085553)

[4.2、其他类账号 17](#_Toc403085554)

[4.3、系统类账号 20](#_Toc403085555)

[5、SAP系统软件设计 23](#_Toc403085556)

[5.1、员工类账号 23](#_Toc403085557)

[5.2、其他类账号 26](#_Toc403085558)

[5.3、系统账号 29](#_Toc403085559)

[5.4、SAP账号参数及角色批量更新 33](#_Toc403085560)

[6、AD系统软件设计 34](#_Toc403085561)

[6.1 员工类账号 34](#_Toc403085562)

[6.2其他类账号 38](#_Toc403085563)

[6.3系统类账号 42](#_Toc403085564)

[7、账号类型更改 45](#_Toc403085565)

[8、账号转移 45](#_Toc403085566)

## 1、文档概述

### 1.1、范围

IAM HER、HEC、TC、SAP、AD系统模块账号管理，主要针对 员工类、系统类和其他类这三类账号的添加，编辑和禁用功能；进行详细的说明；

### 1.2相关文档

《IAM系统日志邮件设计》

数据库设计文档

## 2、E-HR系统软件设计

### 2.1员工类账号

#### 2.1.1、新建员工类账号

1、进入Hr操作员管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



说明

1. 输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工，并给出提示
2. 用户编码，取自AD系统中的域账号登陆名字段
3. 用户名称，取自AD系统中的域账号账号名字段
4. 用户编码、用户名称字段为只读，不可编辑
5. 用户描述、密码级别、生效时间、失效时间、锁定标记、备注、登陆方式 字段都为可编辑
6. 锁定标记 默认不钩选；如果锁定标记勾选，则标记为该用户为禁用；当用户禁用了，相应角色不做处理；

规则

1. 输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且页面所有可填项不可编辑，不继续添加hr操作员信息；
2. 添加员工类账号成功后，将添加日志及发送邮件通知相应管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；
3. 必填项：密码，生效日期；其他为可选项

#### 2.1.2、编辑员工类账号

1、进入HR操作员信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

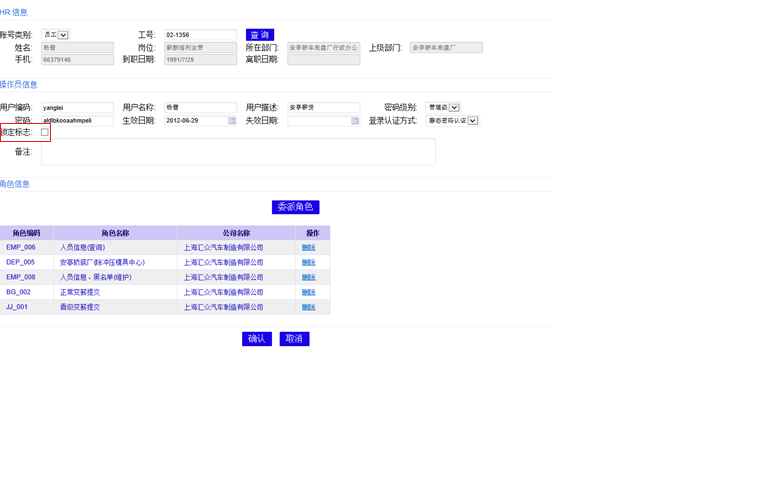
1. 根据HR账号，页面自动展示该用户所有已拥有的信息；
2. 管理员可以更改该页面上的一些信息；
3. 用户描述、密码级别、生效时间、失效时间、锁定标记、备注、登陆方式 字段都为可编辑
4. 用户编码、用户名称不可编辑

规则

1. 失效时间必须大于生效时间；
2. 锁定标记如果勾选，失效时间为必填项；默认失效时间为当前时间；
3. 角色信息列表中的”删除”操作，在点击该按钮，则删除对应的角色信息；但是该删除只是做一次本地删除，并不实际写入数据库；
4. 当管理员点击”确认”按钮，将所有更改的信息更新进数据库；
5. 5、管理员所有的更改都将会记录日志及发送邮件通知相应系统管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；
6. 编辑时，密码项无效；

#### 2.1.3、禁用员工类账号

1、进入HR操作员信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

该页面中的锁定标记字段是控制该账号状态，不勾选为启用，则为禁用；当管理员禁用该账号时，相应角色不做处理；

规则

1. 管理员禁用员工后，将会记录日志及发送邮件通知相应的管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

### 2.2、其他类型账号

#### 2.2.1、新建其他类账号

1、进入Hr操作员管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



说明

1. 输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工，并给出提示
2. 用户编码，唯一命名
3. 用户名称，唯一命名
4. 用户编码、用户名称字段可编辑
5. 用户描述、密码级别、生效时间、失效时间、锁定标记、备注、登陆方式 字段都为可编辑
6. 锁定标记 默认不钩选；如果锁定标记勾选，则标记为该用户为禁用；当用户禁用了，则相应的角色信息不做处理；

规则

1. 输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且不继续添加hr操作员信息；
2. 用户编码、用户名称如果已存在则给予提示，且添加时不给予添加；
3. 日志及邮件格式请参考《IAM系统日志邮件设计》；
4. 必填项：用户名称，用户编码，密码，生效时间；其他为可选项；

#### 2.2.2、编辑其他类账号

1、进入HR操作员信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

1. 根据HR账号，页面自动展示该用户所有已拥有的信息；
2. 管理员可以更改该页面上的一些信息；
3. 用户描述、密码级别、生效时间、失效时间、锁定标记、备注、登陆方式 字段都为可编辑
4. 用户编码、用户名称不可编辑

规则

1. 失效时间必须大于生效时间；
2. 锁定标记如果勾选，默认失效时间为当前时间；
3. 角色信息列表中的”删除”操作，在点击该按钮，则删除对应的角色信息；但是该删除只是做一次本地删除，并不实际写入数据库；
4. 当管理员点击”确认”按钮，将所有更改的信息更新进数据库；
5. 管理员所有的更改都将会记录日志及发送邮件通知相应系统管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；
6. 必填项：用户名称，用户编码，密码，生效时间；其他为可选项；

#### 2.2.3、禁用其他类账号

1、进入HR操作员信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

该页面中的锁定标记字段是控制该账号状态，不勾选为启用，则为禁用；当管理员禁用该账号时，所有的角色信息不做处理；

规则

1. 管理员禁用员工后，将会记录日志及发送邮件通知相应的管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

### 2.3、系统类账号

#### 2.3.1、新建系统类账号

1、进入Hr操作员管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



说明

1. 用户编码，唯一命名
2. 用户名称，唯一命名
3. 用户编码、用户名称字段可编辑
4. 用户描述、密码级别、生效时间、失效时间、锁定标记、备注、登陆方式 字段都为可编辑
5. 锁定标记 默认不钩选；如果锁定标记勾选，则标记为该用户为禁用；当用户禁用了，则相应的角色信息也将被设为禁用及清空；

规则

1. 工号为可选项；如果输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且不继续添加hr操作员信息；
2. 用户编码、用户名称如果已存在则给予提示，且添加时不给予添加；
3. 日志及邮件格式请参考《IAM系统日志邮件设计》；

#### 2.3.2、编辑系统类账号

1、进入HR操作员信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

1. 根据HR账号，页面自动展示该用户所有已拥有的信息；
2. 管理员可以更改该页面上的一些信息；
3. 用户描述、密码级别、生效时间、失效时间、锁定标记、备注、登陆方式 字段都为可编辑
4. 用户编码、用户名称不可编辑

规则

1. 失效时间必须大于生效时间；
2. 锁定标记如果勾选，默认失效时间为当前时间；
3. 角色信息列表中的”删除”操作，在点击该按钮，则删除对应的角色信息；但是该删除只是做一次本地删除，并不实际写入数据库；
4. 当管理员点击”确认”按钮，将所有更改的信息更新进数据库；
5. 管理员所有的更改都将会记录日志及发送邮件通知相应系统管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

#### 2.3.3、禁用系统类账号

1、进入HR操作员信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

该页面中的锁定标记字段是控制该账号状态，不勾选为启用，则为禁用；当管理员禁用该账号时，所有的角色信息都将清空；

规则

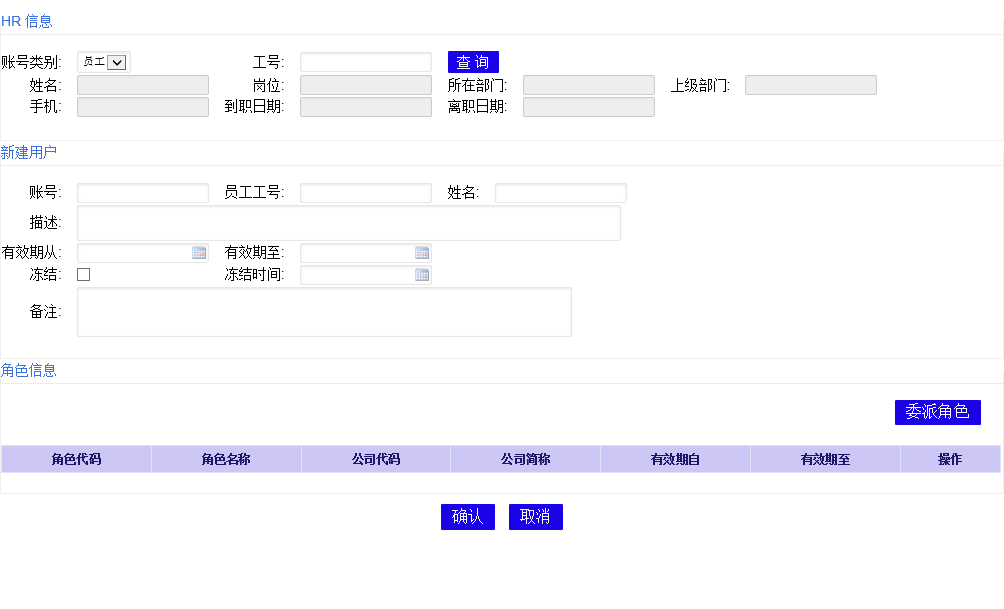
1. 管理员禁用员工后，将会记录日志及发送邮件通知相应的管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

## 3、HEC系统软件设计

### 3.1、员工类账号

#### 3.1.1、新建员工类账号

1、进入HEC操作员管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



说明

1. 输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工；并带出相应hr员工信息
2. 员工代码：员工工号
3. 姓名：Ad系统中账号名
4. 描述：Ad系统中账号名
5. 有效期从：默认为当前时间
6. 有效期至：默认为空，永久

规则

1. 输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且不继续添加HEC操作员信息；

2、添加员工类账号成功后，将添加日志及发送邮件通知相应管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

## TC软件系统设计

### 4.1、员工类账号

#### 4.1.1新建员工类账号

1、进入TC用户信息管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



说明

1. 输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工，并给出提示
2. 用户默认状态为活动
3. 默认工作组、默认角色 这两个字段不可编辑
4. 用户id：根据用户shac+工号自动生成；不可编辑；
5. 操作系统名称：默认为用户id；可编辑
6. Email:不可编辑，在点击查询时，自动带出ad系统中相应的员工类账号信息中email字段；
7. 必填项：人员姓名，用户id，操作系统名称，密码，许可级别，email；其他为可选项；

规则

1. 输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且页面所有可填项不可编辑，不继续添加TC账号信息；
2. 添加员工类账号成功后，将添加日志及发送邮件通知相应管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

#### 4.1.2编辑员工类账号

1、进入TC用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

1. 根据TC账号，页面自动展示该用户所有已拥有的信息；密码字段不做显示；
2. 管理员可以更改该页面上的一些信息；
3. 人员名称，用户id，工号，Email，默认组，默认角色、密码为不可编辑字段；其他字段为可编辑字段；
4. 当用户状态字段，设置为“非活动”时，将默认将账号所有相应的角色及组信息设置为非活动；

规则

1. 当用户状态字段，设置为“非活动”时，将默认将账号所有相应的角色及组信息设置为非活动；
2. 角色信息列表中的”删除”操作，在点击该按钮，则删除对应的角色信息；但是该删除只是做一次本地删除，并不实际写入数据库；
3. 当管理员点击”确认”按钮，将所有更改的信息更新进数据库；
4. 必填项：人员名称、用户id、操作系统名称、许可级别、email、用户状态
5. 可填项：备注
6. 管理员所有的更改都将会记录日志及发送邮件通知相应系统管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；
7. 编辑时，密码项无效；

#### 4.1.3禁用员工类账号

1、进入TC用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

该页面中的用户状态字段是控制该账号状态，选择非活动时则为禁用该账号；当管理员禁用该账号时，相应角色将自动的设置为非活动；

规则

1. 管理员禁用员工后，将会记录日志及发送邮件通知相应的管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

### 4.2、其他类账号

#### 4.2.1新建其他类账号

1、进入TC用户信息管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



说明

1. 输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工，并给出提示
2. 用户默认状态为活动
3. 默认工作组、默认角色 这两个字段不可编辑
4. 用户id：用户自行输入，且是该系统中唯一；
5. 操作系统名称：用户自行输入
6. Email:不可编辑，在点击查询时，自动带出ad系统中相应的员工类账号信息中email字段；
7. 必填项：人员姓名，用户id，操作系统名称，密码，许可级别，email；其他为可选项；

规则

1. 输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且页面所有可填项不可编辑，不继续添加TC账号信息；
2. 添加员工类账号成功后，将添加日志及发送邮件通知相应管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

#### 4.2.2编辑其他类账号

1、进入TC用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

1. 根据TC账号，页面自动展示该用户所有已拥有的信息；密码字段不做显示；
2. 管理员可以更改该页面上的一些信息；
3. 用户id，工号，Email，默认组，默认角色、密码为不可编辑字段；其他字段为可编辑字段；
4. 当用户状态字段，设置为“非活动”时，将默认将账号所有相应的角色及组信息设置为非活动；

规则

1. 当用户状态字段，设置为“非活动”时，将默认将账号所有相应的角色及组信息设置为非活动；
2. 角色信息列表中的”删除”操作，在点击该按钮，则删除对应的角色信息；但是该删除只是做一次本地删除，并不实际写入数据库；
3. 当管理员点击”确认”按钮，将所有更改的信息更新进数据库；
4. 必填项：人员名称、用户id、操作系统名称、许可级别、email、用户状态
5. 可填项：备注
6. 管理员所有的更改都将会记录日志及发送邮件通知相应系统管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；
7. 编辑时，密码项无效；

#### 4.2.3禁用其他类账号

1、进入TC用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

该页面中的用户状态字段是控制该账号状态，选择非活动时则为禁用该账号；当管理员禁用该账号时，相应角色将自动的设置为非活动；

规则

管理员禁用员工后，将会记录日志及发送邮件通知相应的管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

### 4.3、系统类账号

#### 4.3.1、新建系统类账号

1、进入TC用户信息管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



说明

1. 输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工，并给出提示
2. 用户默认状态为活动
3. 默认工作组、默认角色 这两个字段不可编辑
4. 用户id：用户自行输入，且是该系统中唯一；
5. 操作系统名称：用户自行输入
6. Email:不可编辑，在点击查询时，自动带出ad系统中相应的员工类账号信息中email字段；
7. 必填项：人员姓名，用户id，操作系统名称，密码，许可级别，email；其他为可选项；
8. 工号为可选项；如果输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且不继续添加hr操作员信息；

规则

1. 输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且页面所有可填项不可编辑，不继续添加TC账号信息；
2. 添加员工类账号成功后，将添加日志及发送邮件通知相应管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

#### 4.3.2、编辑系统类账号

1、进入TC用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

1. 根据TC账号，页面自动展示该用户所有已拥有的信息；密码字段不做显示；
2. 管理员可以更改该页面上的一些信息；
3. 用户id，Email，默认组，默认角色、密码为不可编辑字段；其他字段为可编辑字段；
4. 当用户状态字段，设置为“非活动”时，将默认将账号所有相应的角色及组信息设置为非活动；

规则

1. 当用户状态字段，设置为“非活动”时，将默认将账号所有相应的角色及组信息设置为非活动；
2. 角色信息列表中的”删除”操作，在点击该按钮，则删除对应的角色信息；但是该删除只是做一次本地删除，并不实际写入数据库；
3. 当管理员点击”确认”按钮，将所有更改的信息更新进数据库；
4. 必填项：人员名称、用户id、操作系统名称、许可级别、email、用户状态
5. 可填项：备注
6. 管理员所有的更改都将会记录日志及发送邮件通知相应系统管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；
7. 编辑时，密码项无效；
8. 工号为可选项；如果输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且不继续添加hr操作员信息；

#### 4.3.3、禁用系统类账号

1、进入TC用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

该页面中的用户状态字段是控制该账号状态，选择非活动时则为禁用该账号；当管理员禁用该账号时，相应角色将自动的设置为非活动；

规则

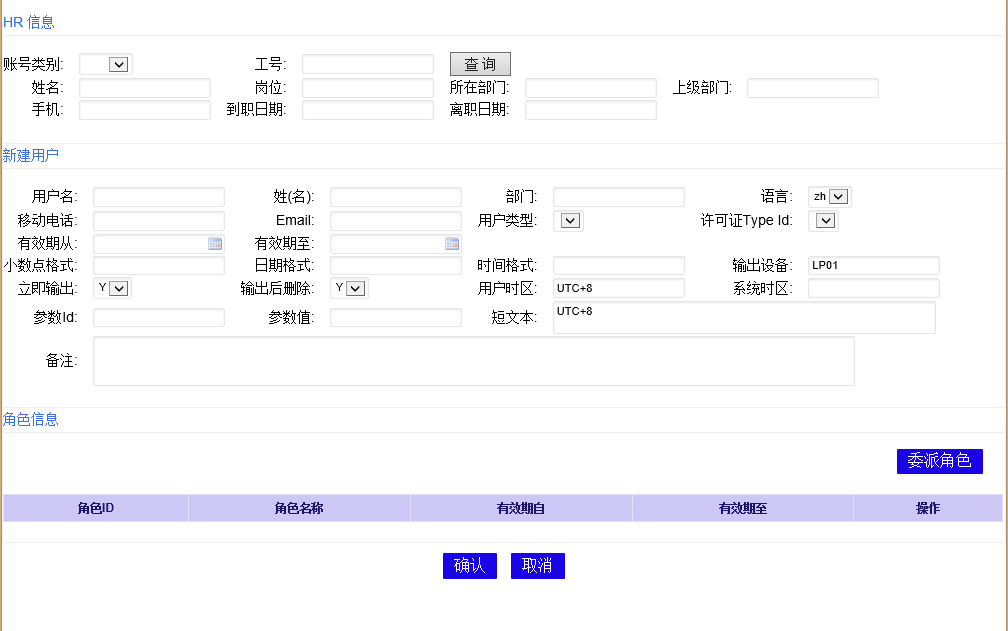
管理员禁用员工后，将会记录日志及发送邮件通知相应的管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

## 5、SAP系统软件设计

### 5.1、员工类账号

#### 5.1.1、新建员工类账号

1、进入SAP用户信息管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



说明

1. 输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工，并给出提示；
2. 点击查询时，自动带出“ 移动电话,email,姓名,部门” 字段信息；且这四个字段是不可编辑；
3. 移动电话：只读显示，不可添加
4. Email：取自ad员工类账号中Email字段
5. 姓名：取自ad员工类账号中账号名字段
6. 部门：只读显示 ，不可添加

规则

1. 输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且页面所有可填项不可编辑，不继续添加SAP操作员信息；
2. 添加员工类账号成功后，将添加日志及发送邮件通知相应管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；
3. 必填项：用户名、姓名、语言、email、用户类型、许可证id、有效期从、日期格式、时间格式、输出设备、立即输出、输出后删除、用户时区、系统时区；
4. 可选项：有效期至、参数id，参数值，短文本，备注、小数点格式、
5. 不填写项：部门、移动电话、
6. 有效期从：默认为当前时间
7. 有效期至：为空为永久，不为空时，则必须大于有效期从字段值
8. 输出设备：默认为” LP01”;
9. 用户时区：默认为”UTC+8”
10. 立即输出：默认为”Y”
11. 输出后删除：默认为”Y”
12. 用户名：根据工号自动生成 格式为SHAC+工号;例如：SHAC011110

#### 5.1.2、编辑员工类账号

1、进入SAP用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

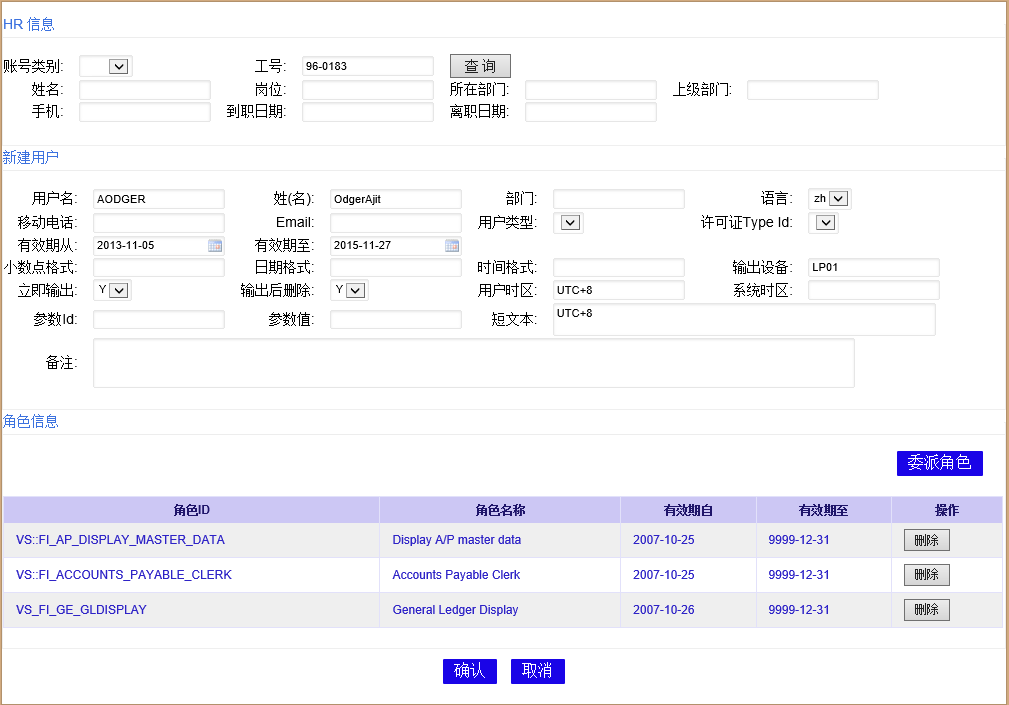
1. 根据SAP账号，页面自动展示该用户所有已拥有的信息；密码字段不做显示；
2. 管理员可以更改该页面上的一些信息
3. 管理员可以编辑更改，语言、有效期从、有效期至、用户类型、许可证id、小数点格式、日期格式、时间格式、输出设备、立即输出、输出后删除、用户时区、系统时区、参数id、参数值、短文本字段；
4. 用户角色信息；
5. 工号、用户名、Email 字段是不可编辑的；
6. 部门、移动电话、只读

规则

1. 角色信息列表中的”删除”操作，在点击该按钮，则删除对应的角色信息；但是该删除只是做一次本地删除，并不实际写入数据库；
2. 当管理员点击”确认”按钮，将所有更改的信息更新进数据库；
3. 必填项：用户名、姓名、部门、语言、移动电话、email、用户类型、许可证id、有效期从、小数点格式、日期格式、时间格式、输出设备、立即输出、输出后删除、用户时区、系统时区；
4. 可选项：有效期至、参数id，参数值，短文本，备注
5. 管理员所有的更改都将会记录日志及发送邮件通知相应系统管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

#### 5.1.3、禁用员工类账号

1、进入SAP用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

当管理员将有效期至设置为当前时，则该用户为禁用账号；且在禁用时，将员工所相应的角色有效期至字段设置为当前时间；在禁用账号时，且记录更改的字段；

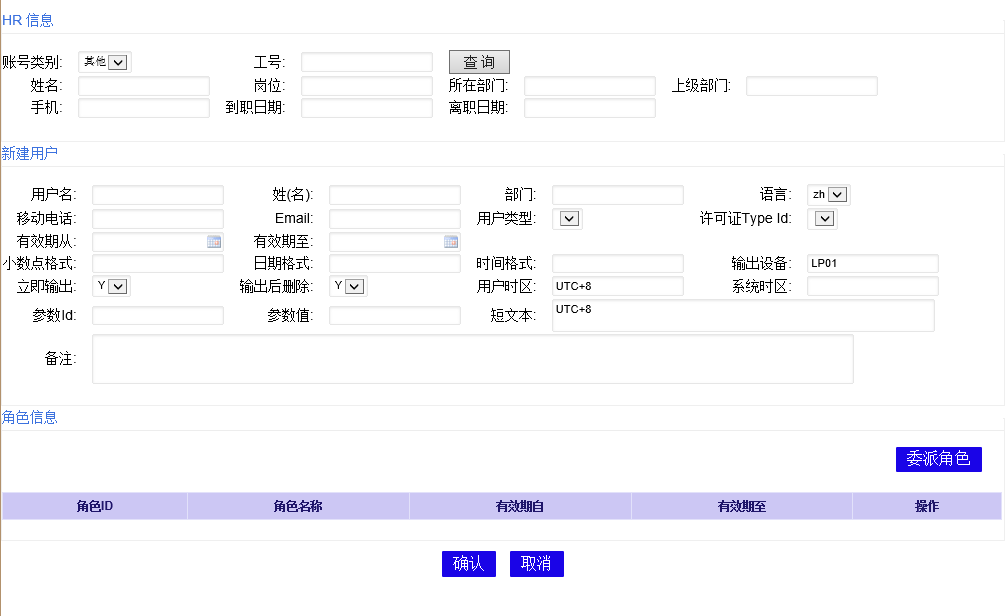
规则

管理员禁用员工后，将会记录日志及发送邮件通知相应的管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

### 5.2、其他类账号

#### 5.2.1、新建其他类账号

1、进入SAP用户信息管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



说明

1. 输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工，并给出提示；
2. 用户名：系统唯一

规则

1. 输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且页面所有可填项不可编辑，不继续添加SAP操作员信息；
2. 添加员工类账号成功后，将添加日志及发送邮件通知相应管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；
3. 必填项：用户名、语言、用户类型、许可证id、有效期从、小数点格式、日期格式、时间格式、输出设备、立即输出、输出后删除、用户时区、系统时区；
4. 可选项：有效期至、参数id、参数值、短文本、备注、姓名、部门、移动电话、email
5. 有效期从：默认为当前时间；
6. 有效期至：为空为永久，不为空时，则必须大于有效期从字段值；
7. 输出设备：默认为” LP01”；;
8. 用户时区：默认为”UTC+8”；
9. 立即输出：默认为”Y”；
10. 输出后删除：默认为”Y”；
11. 用户名：系统唯一，如果输入的用户名已存在则给予提示，且将不可添加；

#### 5.2.2、编辑其他类账号

1、进入SAP用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

1. 根据SAP账号，页面自动展示该用户所有已拥有的信息；密码字段不做显示；
2. 管理员可以更改该页面上的一些信息
3. 管理员可以编辑更改，语言、有效期从、有效期至、用户类型、许可证id、小数点格式、日期格式、时间格式、输出设备、立即输出、输出后删除、用户时区、系统时区、参数id、参数值、短文本字段、部门、移动电话、Email；
4. 用户角色信息；
5. 工号、用户名、字段是不可编辑的；

规则

1. 角色信息列表中的”删除”操作，在点击该按钮，则删除对应的角色信息；但是该删除只是做一次本地删除，并不实际写入数据库；
2. 当管理员点击”确认”按钮，将所有更改的信息更新进数据库；
3. 必填项：用户名、用户类型、许可证id、有效期从、小数点格式、日期格式、时间格式、输出设备、立即输出、输出后删除、用户时区、系统时区；
4. 可选项：有效期至、参数id，参数值，短文本，备注、姓名、部门、语言、移动电话、email；
5. 管理员所有的更改都将会记录日志及发送邮件通知相应系统管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

#### 5.2.3、禁用其他类账号

1、进入SAP用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

当管理员将有效期至设置为当前时，则该用户为禁用账号；且在禁用时，将员工所相应的角色有效期至字段设置为当前时间；

规则

管理员禁用员工后，将会记录日志及发送邮件通知相应的管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

### 5.3、系统账号

#### 5.3.1、新建系统账号

1、进入SAP用户信息管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



说明

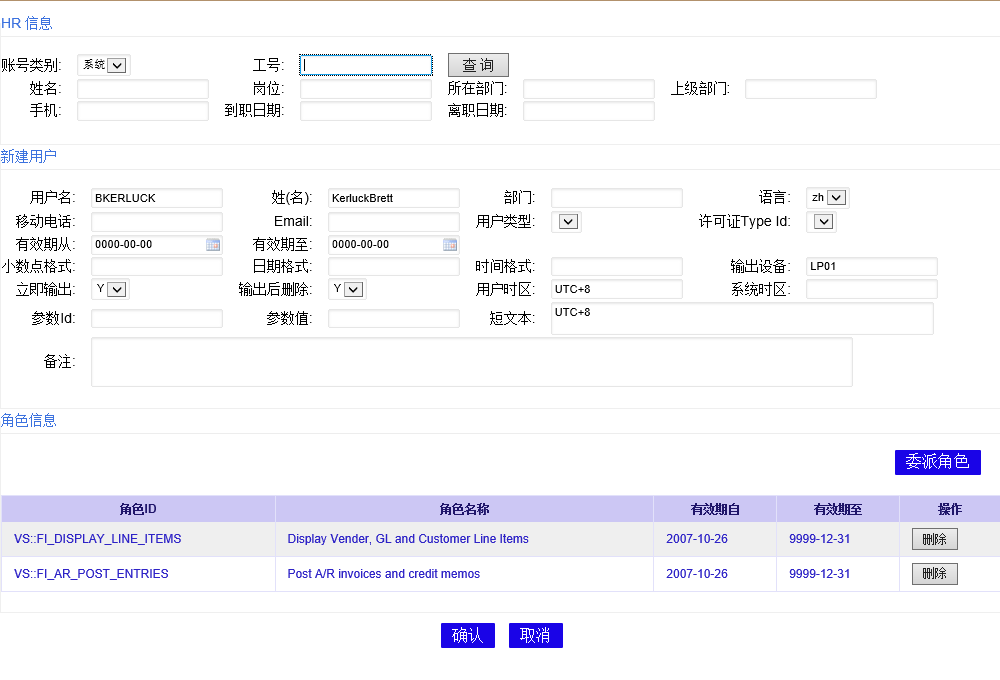
该页面上的所有字段，在添加时都是为可编辑的；用户名为管理员自行输入且在sap系统中为唯一的；

规则

1. 工号字段为可选项，如果输入工号，点击查询后，仅显示在职且在AD系统中已存在该工号对应的员工类ad账号；如果没有ad员工类账号则给予提示，并且页面所有可填项不可编辑，不继续添加SAP操作员信息；
2. 添加员工类账号成功后，将添加日志及发送邮件通知相应管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；
3. 必填项：用户名、语言、用户类型、许可证id、有效期从、小数点格式、日期格式、时间格式、输出设备、立即输出、输出后删除、用户时区、系统时区；
4. 可选项：有效期至、参数id、参数值、短文本、备注、姓名、部门、移动电话、email
5. 有效期从：默认为当前时间；
6. 有效期至：为空为永久，不为空时，则必须大于有效期从字段值；
7. 输出设备：默认为” LP01”；;
8. 用户时区：默认为”UTC+8”；
9. 立即输出：默认为”Y”；
10. 输出后删除：默认为”Y”；
11. 用户名：系统唯一，如果输入的用户名已存在则给予提示，且将不可添加；

#### 5.3.2、编辑系统类账号

1、进入SAP用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

1. 根据SAP账号，页面自动展示该用户所有已拥有的信息；密码字段不做显示；
2. 管理员可以更改该页面上的一些信息
3. 管理员可以编辑更改，语言、有效期从、有效期至、用户类型、许可证id、小数点格式、日期格式、时间格式、输出设备、立即输出、输出后删除、用户时区、系统时区、参数id、参数值、短文本字段、部门、移动电话、Email；
4. 用户角色信息；
5. 工号、用户名、字段是不可编辑的；

规则

1. 角色信息列表中的”删除”操作，在点击该按钮，则删除对应的角色信息；但是该删除只是做一次本地删除，并不实际写入数据库；
2. 当管理员点击”确认”按钮，将所有更改的信息更新进数据库；
3. 必填项：用户名、用户类型、许可证id、有效期从、小数点格式、日期格式、时间格式、输出设备、立即输出、输出后删除、用户时区、系统时区；
4. 可选项：有效期至、参数id，参数值，短文本，备注、姓名、部门、语言、移动电话、email；
5. 管理员所有的更改都将会记录日志及发送邮件通知相应系统管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

#### 5.3.3、禁用系统类账号

1、进入SAP用户信息管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



说明

当管理员将有效期至设置为当前时，则该用户为禁用账号；且在禁用时，将员工所相应的角色有效期至字段设置为当前时间；

规则

管理员禁用员工后，将会记录日志及发送邮件通知相应的管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

### 5.4、SAP账号参数及角色批量更新

1、进入SAP菜单，在SAP菜单下，点击“sap批量工具”，进入如下图页面：



图sap01-1

说明

该页面主要有两个功能：

1. 用户账号的Id，参数值，短文本 字段的批量更新
2. 用户账号的角色，批量添加及删除

规则

1. 账号字段不能为空，不能自行填写；必须进入如下页面选择；



1. 参数Id、参数值、短文本 字段不能为空；
2. 角色的批量添加及删除，必须进入如下页面选择：



1. 上图中选择号角色后，添加”确定”按钮后，效果图如 “图sap01-1”中显示；在“图sap01-1”角色列表中，最后一列“操作”列中，有”添加”，“删除”两个选项；默认添加选项为勾选的；当选择添加项时，则向选择的账号添加该角色；当选择删除项时，则将选择的账号删除已拥有的该角色信息；
2. 管理员所有的更改都将会记录日志及发送邮件通知相应系统管理员；日志及邮件格式请参考《IAM系统日志邮件设计》；

## 6、AD系统软件设计

### 6.1 员工类账号

#### 6.1.1添加员工类账号

1、进入ad账号管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



2、说明

1、输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工，并给出提示；  
  
2、ad模快信息中，"enable"字段默认是启用；  
  
3、ad模快信息中，"CN"字段默认自动带出，该字段来自hr员工信息中中文名字段，在添加时判断ad系统是否已存在重复，如果存在重复则自动给该字段后面添加编号，如：张三1  
  
4、ad模快信息中,"描述"字段根据IAM管理员选择组信息时，判断出该员工所在的ad部门；在根据ad部门字段去部门工作组信息表中，带出department，center，科室；三个字段组成描述；  
  
5、ad模快信息中，新增一"邮箱数据库"字段，用来存储账号员工类账号，邮件存放的邮件数据库；  
  
6、ad模快信息中，" 职务级别"字段，由现在的手动输入该为下拉框选择；   
  
7、ad模快信息中，"Email"、"Lync"两个字段；当选择账号类型为"员工类"或"其他类型"时，这两个字段是根据是根据用户填写的"登陆名"自动生成且不可编辑；   
  
8、在新建员工类账号时，管理员填写完”登录名”后，自动生成計算機账号信息且计算机名称跟登录名相同；  
  
9、ad模快信息中，"密码"字段在新建时可以编辑并以明文形式保存进系统；但是在更新、查看账号信息时该字段是不能编辑且不可查看；  
  
10、ad模快信息中， "最后登陆时间"、 "密码变更时间"两个字段；最后登陆时间，密码变更时间均来自接口，所以在新建账号时这两个字段不显示，在查看时才给予显示；

11、在添加計算機账号时，先添加計算機信息；計算機信息添加成功后，去計算機管理页面中给新加的計算機添加工作组信息；

12. 去掉邮箱大小

13，人员类型改为账号类型

14，在切换账号类型是提示确认框，确认框内容为“是否确认变更账号类型,如果变更会引起当前编辑内容丢失！”

15，如果当前选择的用户已经存在关联的员工类域账号，则提示“已经存在员工类域账号，不能添加员工类域账号”。

16，在页面刚打开时，只有账号类型和工号可编辑，当用户输入有效的工号时（点击查询之后）将其他需要编辑的字段置为可编辑状态

17，部门改为下拉模式，下拉数据来自维护的部门工作中维护的部门，当用户选择了部门之后，自动添加部门工作组

18，工作组分多个table实现，（默认工作组，部门工作组，职级工作组，可控工作组）

3、规则  
  
1、ad模快信息中，"用户名"， "登陆名"， "显示名"在ad系统中都是唯一性的；所以在新建时需要验证其唯一性；如果遇到重复，则需要在用户名，登陆名，CN后面添加序号，再保存时验证显示名是否重复，如果重复则提示用户修改显示名；  
  
2、在添加ad账号时，如果账号类型选择为"其他类型"，输入工号查询后，ad模快信息将手动填写信息；并不根据工号带出hr信息及相应ad相关信息；并且工号是必须填写字段；且其他类型账号中，部门工作组没有默认工作组，所以需手动选择工作组信息；

#### 61.2编辑员工类账号

1、进入ad账号管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：

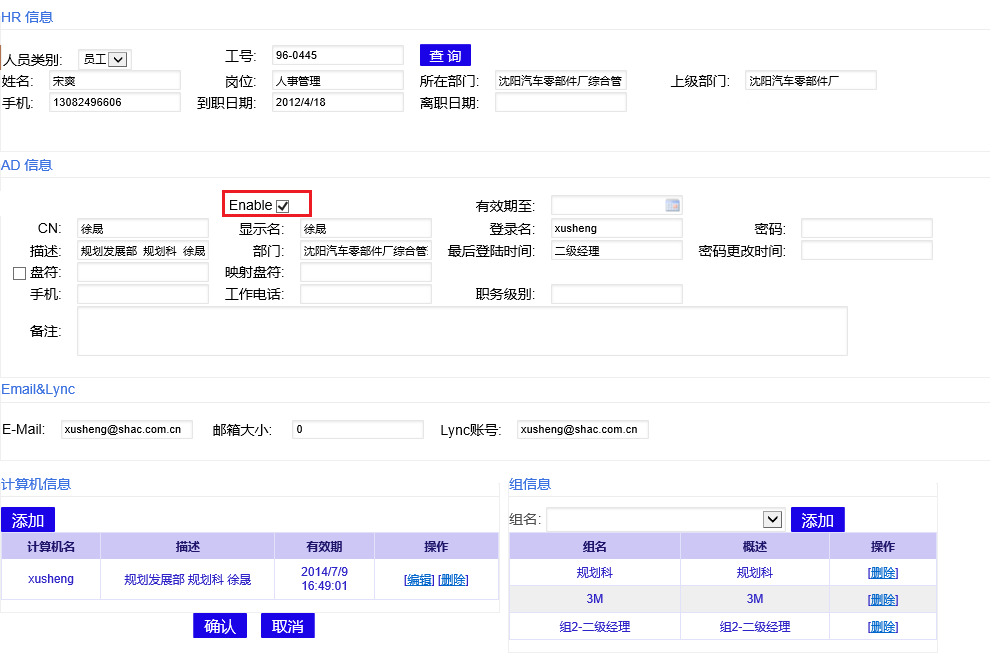


2、说明

1. 根据ad账号，页面自动展示该用户所有已拥有的信息；
2. 管理员可以更改该页面上的一些信息；
3. 可编辑信息由用户的“组信息（默认组，职级组，默认部门编辑），手机，工作电话，备注，盘符，职务级别、有效期、邮箱数据库，部门，启用状态”字段；
4. 编辑时密码字段不显示
5. 规则
6. 跟登录名相同的计算机账号是不能删除的；且该计算机的信息是不能手动编辑的；
7. 组信息中，管理员是可以给该账号添加可控组，部门组权限的；
8. 计算机信息中，”添加”、”编辑”按钮是打开新的计算机详细页面，在新页面中编辑和添加新的计算机账号信息；
9. Hr信息中，所有信息均不可编辑
10. 当前职级变更时，自动变更对应的职级组信息
11. 当部门变更时，自动变更对应的部门组信息，并且域账号描述，计算机描述需要自动更新，自动的数据不能删除

#### 6.1.3禁用员工类账号

1、进入ad账号管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



2、说明

该页面中的Enable字段是控制该账号状态，即为启用还是禁用；当管理员禁用该账号时，所有的组信息都将清空,相同登录名计算机账号被禁用，非相同登录名计算机账号将不被禁用；

3、规则

1、当管理员在禁用用户，在点击确认按钮时，给予”当用户禁用后，所有的组信息和计算机信息都将清空，是否确认禁用该用户？”警告；

2、当管理员点击警告上的确认按钮才真正给予删除；

3、当管理员点击警告上的取消按钮将不给予删除；

4、清空组信息和计算机信息都是在点击取人按钮后才给予操作；

5、禁用域账号之前，首先检查该域账号所对应的工号在其他系统中存在账号，如果存在则先禁用其他系统中该账号，然后方可禁用ad系统该域账号；

### 6.2其他类账号

#### 6.2.1添加其他类账号

1、进入ad账号管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



2、说明

1、管理员首先选择其他类别，在输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工，并给出提示；  
  
2、ad模快信息中，"enable"字段默认是启用；  
  
3、ad模快信息中，"CN"、显示名、登录名、字段都可手动输入，验证唯一性；不是唯一则由管理员手动更改；   
4、ad模快信息中,"描述"字段根据IAM管理员选择组信息时，判断出该员工所在的ad部门；在根据ad部门字段去部门工作组信息表中，带出department，center，科室；三个字段组成描述；  
  
5、ad模快信息中，" 职务级别"字段，由现在的手动输入该为下拉框选择；并且在选择好职务级别后，自动带出"邮件数据库大小"字段值；下拉列表中的来自管理员配置的职级表中；  
  
6、ad模快信息中，"Email"、"Lync"两个字段；根据”是否生成”checkbox是否选中，如果选中则根据登录名自动生成且不可编辑，否则不自动生成；  
7、添加其他类时，不能添加計算機账号；  
  
8、ad模快信息中，"密码"字段在新建时可以编辑并以明文形式保存进系统；但是在更新、查看账号信息时该字段是不能编辑且不可查看；  
  
9、ad模快信息中， "最后登陆时间"、 "密码变更时间"两个字段；最后登陆时间，密码变更时间均来自接口，所以在新建账号时这两个字段不显示，在查看时才给予显示；

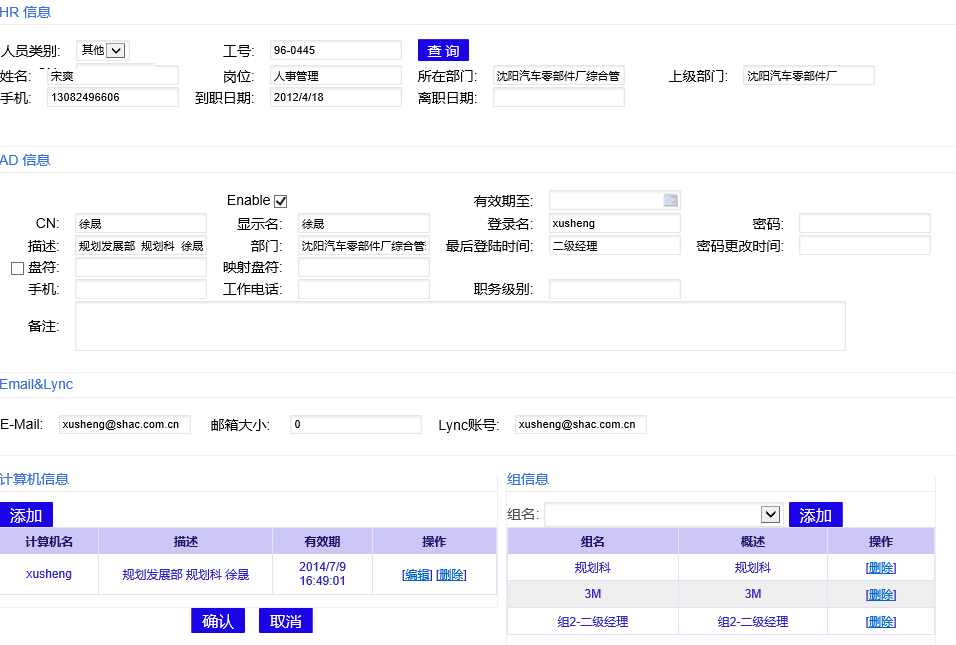
10、添加其他类账号时，不自动添加计算机账号   
11、如果添加计算机账号，则点击添加按钮，在新页面中添加计算机信息；

3、规则

1、ad模快信息中，"用户名"， "登陆名"， "显示名"在ad系统中都是唯一性的；所以在新建时需要验证其唯一性；如果遇到重复，则手动变更；  
  
2、在添加ad账号时，如果账号类型选择为"其他类型"，工号是必须填写字段；且其他类型账号中，部门工作组没有默认工作组，所以需手动选择工作组信息；

#### 6.2.2编辑其他类账号

1、进入ad账号管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



1. 说明

1、根据ad账号，页面自动展示该用户所有已拥有的信息；

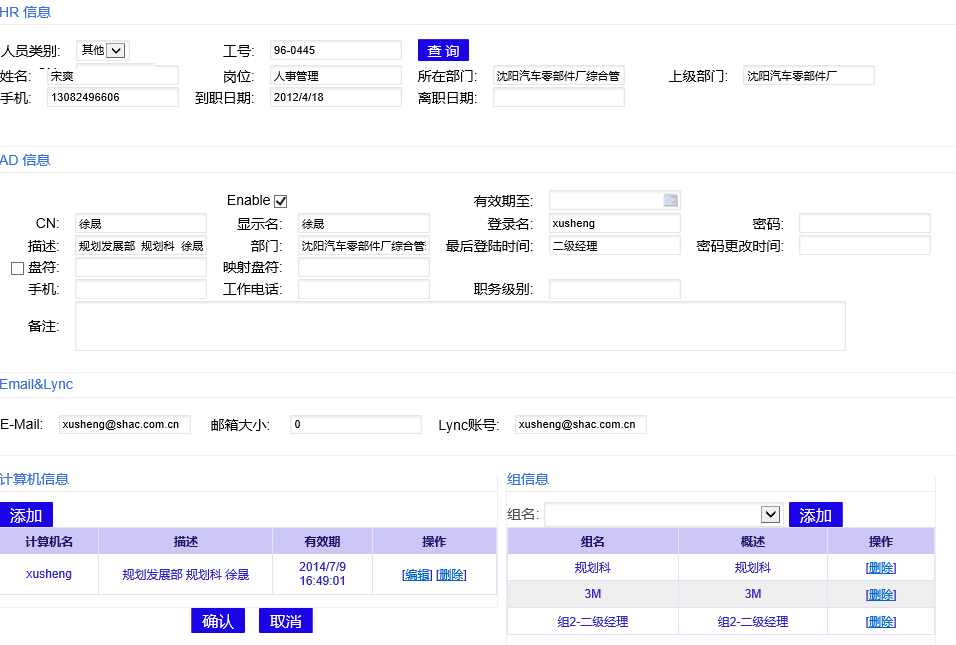
2、管理员可以更改该页面上的一些信息；

3、可编辑信息由用户的所在组信息，计算机账号，手机，工作电话，备注，盘符，职务级别、有效期、邮箱大小字段；

1. 规则
2. 工号不可编辑
3. 员工登录名，CN不能编辑
4. 显示名可编辑
5. 用户账号在编辑下是不显示密码的
6. Hr信息中，所有信息均不可编辑
7. 其他类账号，在填写登录名时不自动生成计算机账号信息
8. 计算机信息中，”添加”、”编辑”按钮是打开新的计算机详细页面，在新页面中编辑和添加新的计算机账号信息；

#### 6.2.3禁用其他类账号

1、进入ad账号管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



2、说明

该页面中的Enable字段是控制该账号状态，即为启用还是禁用；当管理员禁用该账号时，所有的组信息和非相同登录名都将清空；

3、规则

1、当管理员在禁用用户，在点击确认按钮时，给予”当用户禁用后，所有的组信息和计算机信息都将清空，是否确认禁用该用户？”警告；

2、当管理员点击警告上的确认按钮才真正给予删除；

3、当管理员点击警告上的取消按钮将不给予删除；

4、清空组信息和计算机信息都是在点击取人按钮后才给予操作；

### 6.3系统类账号

#### 6.3.1添加系统类账号

1、进入ad账号管理页面，在页面上点击”新建用户”按钮，进入如下图页面：



2、说明

0、管理员首先选择系统类别；可以不输入工号   
  
1、管理员首先选择其他类别，在输入工号，点击查询按钮后，仅显示在职员工账号信息，过滤离职员工，并给出提示；  
  
2、ad模快信息中，"enable"字段默认是启用；  
  
3、ad模快信息中，"CN"、显示名、登录名、字段都可手动输入，验证唯一性；不是唯一则由管理员手动更改；   
4、ad模快信息中,"描述"字段根据IAM管理员选择组信息时，判断出该员工所在的ad部门；在根据ad部门字段去部门工作组信息表中，带出department，center，科室；三个字段组成描述；  
  
5、ad模快信息中，" 职务级别"字段，由现在的手动输入该为下拉框选择；并且在选择好职务级别后，自动带出"邮件数据库大小"字段值；下拉列表中的来自管理员配置的职级表中；  
  
6、ad模快信息中，"Email"、"Lync"两个字段；根据”是否生成”checkbox是否选中，如果选中则根据登录名自动生成且不可编辑，否则不自动生成；  
7、在新建员工类账号时，管理员填写完”登录名”后，自动生成計算機账号信息且计算机名称跟登录名相同；  
  
8、ad模快信息中，"密码"字段在新建时可以编辑并以明文形式保存进系统；但是在更新、查看账号信息时该字段是不能编辑且不可查看；  
  
9、ad模快信息中， "最后登陆时间"、 "密码变更时间"两个字段；最后登陆时间，密码变更时间均来自接口，所以在新建账号时这两个字段不显示，在查看时才给予显示；

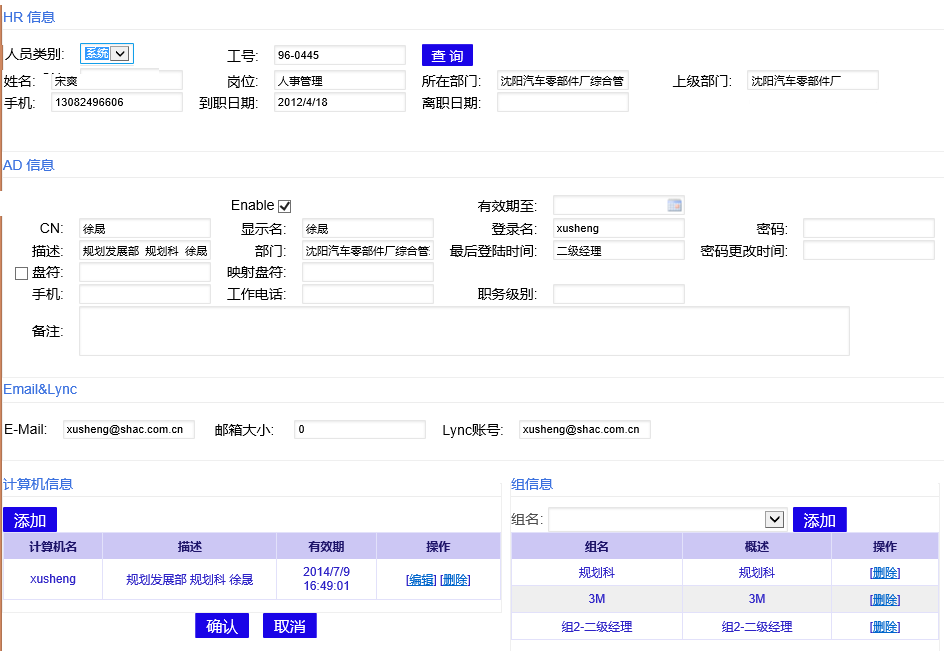
10、添加其他类账号时，不自动添加计算机账号   
11、如果添加计算机账号，则点击添加按钮，在新页面中添加计算机信息；

3、规则

1、ad模快信息中，"用户名"， "登陆名"， "显示名"在ad系统中都是唯一性的；所以在新建时需要验证其唯一性；如果遇到重复，则需要在用户名，登陆名，显示名后面添加序号；  
  
2、在添加ad账号时，如果账号类型选择为"系统"，可以不用输入工号，ad模快信息将手动填写信息；   
3、在添加ad账号时，如果账号类型选择为"系统类型"，工号可以不输入，hr信息可以不填写；且Email，lync账号可以不自动生成，但可编辑；

#### 6.3.2编辑系统类账号

1、进入ad账号管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



2、说明

1、根据ad账号，页面自动展示该用户所有已拥有的信息；

2、管理员可以更改该页面上的一些信息；

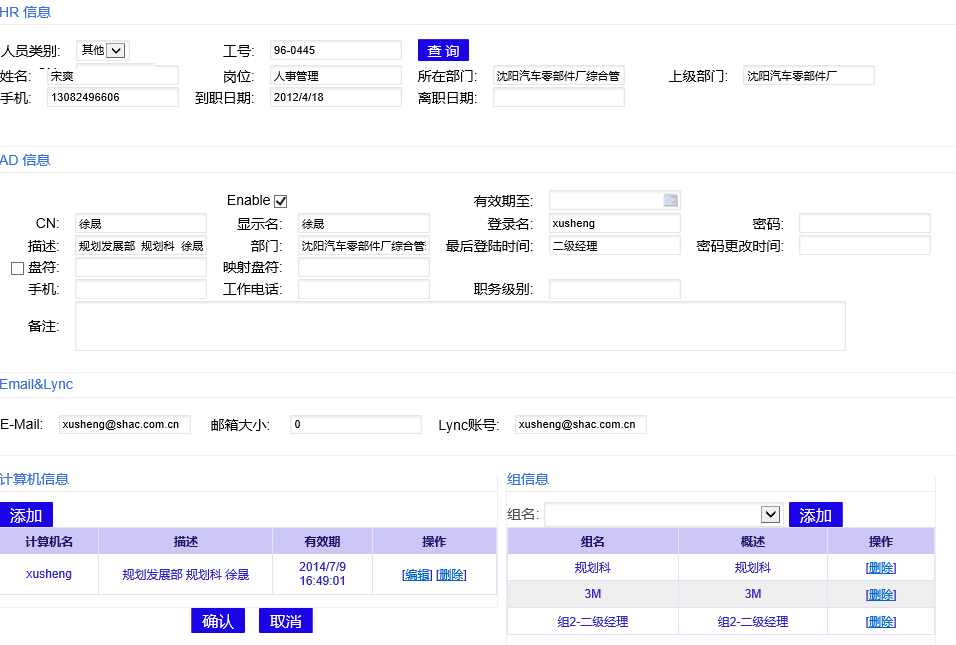
3、可编辑信息由用户的所在组信息，计算机账号，手机，工作电话，备注，盘符，职务级别、有效期、邮箱大小字段；

3、规则

1. 工号不可编辑
2. 员工登录名，CN不能编辑
3. 显示名可编辑
4. 用户账号在编辑下是不显示密码的
5. Hr信息中，所有信息均不可编辑
6. 其他类账号，在填写登录名时不自动生成计算机账号信息
7. 计算机信息中，”添加”、”编辑”按钮是打开新的计算机详细页面，在新页面中编辑和添加新的计算机账号信息；

#### 6.3.3禁用系统类账号

1、进入ad账号管理页面，在页面用户列表中点击”编辑”按钮，进入如下图页面：



2、说明

该页面中的Enable字段是控制该账号状态，即为启用还是禁用；当管理员禁用该账号时，所有的组信息和非相同登录名都将清空；

3、规则

1、当管理员在禁用用户，在点击确认按钮时，给予”当用户禁用后，所有的组信息和计算机信息都将清空，是否确认禁用该用户？”警告；

2、当管理员点击警告上的确认按钮才真正给予删除；

3、当管理员点击警告上的取消按钮将不给予删除；

1. 清空组信息和计算机信息都是在点击取人按钮后才给予操作；

## 7、账号类型更改

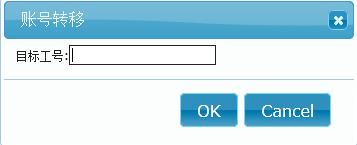
各个系统中的账号类型分别为 员工，其他，系统 三种类型；其这三种类型都可以更改；其中员工类账号可以更改为其他类或系统类；但其他类和系统类则不可更改为员工类；其他类和系统类这个两种类型可以互换；如果系统类或其他类更改为员工类时，系统会给予提示，且类型保持原类型不变；系统

## 8、账号转移

在各个系统的账号列表中，都会有如下图所示的“转移”按钮：



当该账号类型为其他类或系统类时，则显示”转移”按钮;点击转移按钮会出现如下页面：



填写转移目标工号即可完成账号转移；且会记录日志；

日志格式参考日志格式请参考《IAM系统日志邮件设计》；