密码策略

1. 描述

在活字格中，创建用户时设置的密码至少包含六个字符，必须是字母、数字或符号。

默认创建用户时的密码比较简单，他人能够轻易的猜到或破解密码，会造成安全隐患。为了防止这一隐患，您可以设置密码策略，让用户使用更复杂、更安全的密码。

2. 密码策略

以在管理控制台设置密码策略为例，来介绍密码策略的设置及应用。

进入管理控制台，单击“设置”，选择密码策略，进入密码策略设置页面。

图1　密码策略设置

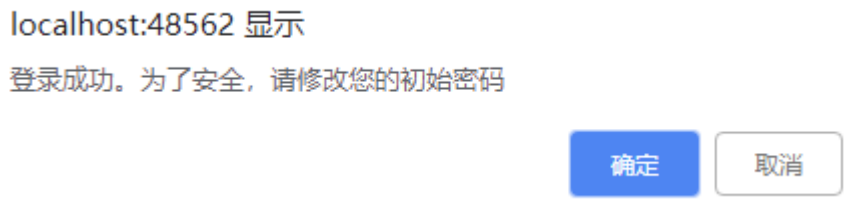
基本设置

基本设置包括以下两项，您可以只勾选其中一项，也可以同时勾选这两项。

- 如果用户没有修改过初始密码，则在其登录时，提醒用户修改密码。

勾选此项后，如果用户没有修改过初始密码，则在其登录时，会弹出如图所示对话框，提醒用户修改密码。

图2　提示修改密码



单击“确定”后，就会跳转到内建页面修改密码页面，如下图所示。

图3　修改密码

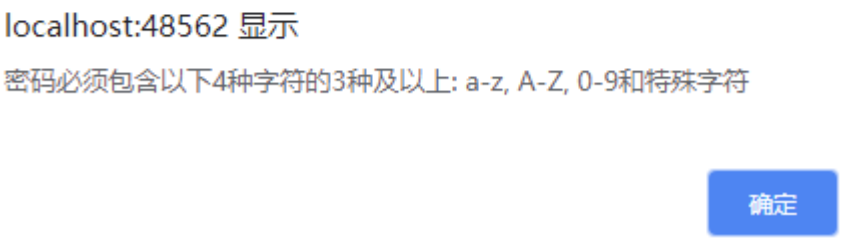
- 使用高强度的密码，即密码长度为8-18位，且至少包含下列4种字符中的3种：
  - 小写字母 a-z；
  - 大写字母 A-Z；
  - 数字 0-9；
  - 特殊字符 @ # $ % ^ & * - _ ! + = [ ] { } | : ‘ , . ? / ` ~ ″ ( ) ；

勾选此项后，修改密码时，新密码必须满足要求，如新密码不满足要求，则会弹出如下提示：

图4　密码错误提示

密码长度不满足要求时，提示如下：

密码复杂度不满足要求时，提示如下：



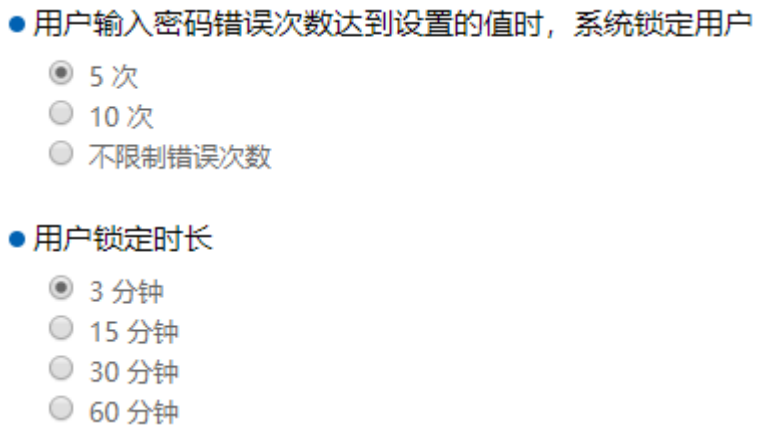
密码输入错误后的限制策略

用户输入密码错误次数达到设置的值时，系统将锁定用户。可选择5次、10次或不限制错误次数。

选择5次或10次时，您还可以设置用户锁定时长，包括3分钟、15分钟、30分钟和60分钟。

例如，选择错误次数为5次，锁定时长为3分钟，则当用户登录系统时，密码输入错误5次后系统将锁定用户，3分钟后会将用户解锁，用户可重新输入密码进行登录。

图5　密码输入错误后的限制策略



回到顶部