权限平台优化需求文档2024.06.M1版

**1. 文档综述**

**1.1版本修改记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 修订内容 | 更改人 | 审批人 | 更改日期 |
| .0 | 配合等保要求，系统安全性增强 | 陈昕 | 刘冬冬 | 2024.05.31 |

**1.2 输出环境**

|  |  |
| --- | --- |
| 需求文档名称 | 权限平台优化需求文档2024.06.M1版本 |
| 版本 | .0 |
| 撰写时间 | 2024.05.27 |
| 撰写人 | 陈昕 |

**1.3 优化简介**

1、IP地址校验：可以设置企业级IP黑白名单，不符合要求的用户IP地址无法登录该企业。

2、密码登录安全加强：密码默认90天密码过期（等保要求），IP地址变化时需要短信二次校验。

**2. 全局说明**

1. 文档中的图片，如果是进行了UI设计的部分则直接是UI设计稿，没有进行UI设计的部分为原型图。
2. 如果是在原来的页面上改动，则改动的地方会以橙色方框圈出，方便辨识。
3. 重点内容文字用橙色字体表示。
4. **详细设计说明**
   1. **IP地址校验**

在客户管理页面的企业列表，企业操作菜单增加“企业级权限”菜单项，如下图所示：



此菜单用来管理针对企业级的权限配置，对该企业下所有用户都生效，对外部联系人不生效。

点击“企业级权限”菜单弹出“企业级权限”配置对话框，如下图所示：



该对话框目前只有一个“用户IP过滤”选项，默认为无过滤IP，登录时不做IP过滤；

用户可以同时添加白名单和黑名单，如下图所示：



点击“添加”按钮可以新增IP输入框。输入框placeholder为“请输入IPV4地址，可以用子网掩码的格式来匹配IP地址段”。点击“删除”可删除输入框，不论输入框内是否有内容输入，都是直接删除。

点击“保存”按钮只保存，保存成功以后不关闭对话框，只弹出toast提示“保存企业级权限成功”，点击“保存并关闭”按钮保存成功后弹出toast提示并关闭对话框。

保存提交前需要进行如下操作：

Step1：校验每个输入框是否有内容填写，如果有未填写的，在该输入框下面出现红字“请输入IP地址或地址段”。

Step2：校验每个输入框内的IP地址必须符合IPV4格式，即“<num>.<num>.<num>.<num>”其中“<num>”为0-255的整数。也可以为“<num>.<num>.<num>.<num>/<匹配二进制位数>”此时为按照子网掩码格式匹配IP地址段，例如“183.23.112.18”是匹配该IP地址，“183.23.112.0/24”匹配“183.23.112.0”-“183.23.112.255”地址段。如果有格式错误或一个输入框内输入了多个IP地址的，在该输入框下面出现红字“IP地址或地址段格式错误”。

Step3：提交前自动过滤IP地址前后的“空格”字符。对于多个输入框输入相同的IP地址、输入相同的IP地址段、IP地址包含在IP地址段内的情况，由于实际很少会发生，前端无需做过滤，后端需要过滤下，对于输入相同的IP地址或地址段的只保留一个即可，IP地址包含在IP地址段内的去掉IP地址。

设置好IP地址并保存后，登录时先按照原有的流程校验登录是否通过（密码是否正确or短信验证码是否正确or米度云扫描是否成功or微信扫码是否成功，密码登录校验具有更复杂的逻辑，详见3.2.2），登录校验通过以后校验当前登录用户的IP是否符合要求，如果IP校验通过则正常登录如果不通过则登录失败停留在登录页面提示“登录失败，用户IP地址异常！”。对于统一登录页、MDNET2.0、米度云、米易通都按此逻辑。

如果之前配置了IP过滤，再次配置时需要把之前的配置带出来。

* 1. **密码登录安全加强**

**3.2.1密码设置优化**

在新增用户和修改密码对话框保存校验时，校验规则由原来的15-30位降低到8-30位，其他的不变，如果校验不通过，提示“密码需要为8-30位字符，至少同时包含大小写字母、数字以及特殊符号\_!@#¥%^&\*之一”。











在修改时需要校验新密码和原密码是否相同，如果相同在保存时弹出错误提示语“原密码和新密码不能相同”，且无法保存。

**3.2.2密码登录校验优化**

在使用密码登录时，需要按照如下顺序校验：

Step1：校验密码是否正确，如果错误则提示“用户名或密码错误”且登录失败，停留在登录页面不动，如果校验通过进入Step2。

Step2：如果设置了IP白名单或黑名单，需要校验IP是否合规，不合规提示“登录失败，用户IP地址异常！”且登录失败，停留在登录页面不动，合规则进入Step3。

Step3：校验当前IP是否在最近10次登录（任何登录方式）的IP内（如果从账号注册后登录不足10次则校验是否在前面登录的所有IP地址内）。如果校验不通过，则弹出短信验证对话框，如下图所示：



此时在后端自动匹配当前账号对应的手机号，其他交互逻辑同短信验证登录，提示语原文：“点击“获取验证码”将向您注册的手机号发送验证码”。此对话框没有关闭按钮也不能点击页面其他位置消失，在规定的时间内短信验证通过则登录成功，验证不通过则无法登录。APP也要参照PC端做一个短信二次校验页面，且隐藏真实手机号码。

如果校验通过则进入Step4。

Step4：校验密码是否过期，如果此刻超过此密码设置的时间90天，则弹出toast提示“密码超过90天有效期，请重新设置密码”，且弹出密码快捷设置对话框：



获取验证码流程参考验证码登录，输入新密码需要校验密码格式和两次输入是否一致，交互参考权限平台改密功能。密码输入框需要有显隐开关，默认隐藏字符用点代替。新密码保存成功以后toast提示“密码修改成功”并且对话框消失。用户可以输入新密码重新登录。此步骤，如果是APP登录则过期时直接弹出错误toast提示“密码已过90天有效期，请更新密码”，且登录失败。

如果未过期则登录成功。

对于统一登录页、MDNET2.0、米度云、米易通都按此逻辑。