关于 OA 产品弱口令防范的加固措施建议

一、弱口令防范的基本要求

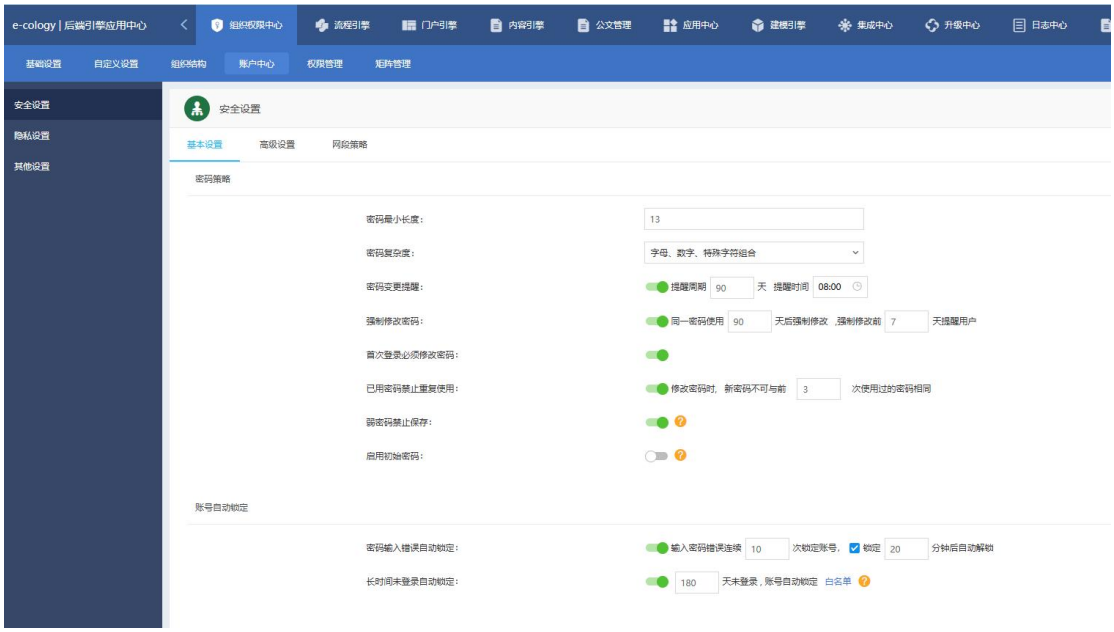
1、密码复杂度要求

a、长度至少 13 位及以上；
b、同时包含大小写字母、数字和特殊字符；
c、在键盘上没有明显的输入规律，比如：1qaz@WSX，比如该密码，看似是强密码，但在键盘上存在明显输入规律，因此也容易破解。

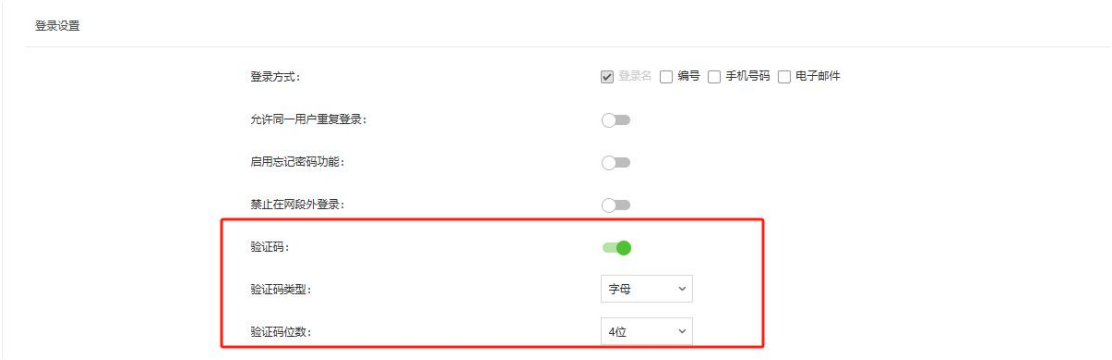
2、定期修改密码（建议最长 90 天变更一次密码），且不能与前 3 次密码一样。不同系统的密码应避免使用相同的密码。

二、Ecology9.0 产品口令配置策略建议

1、建议按照下图中的方式配置系统口令复杂度：



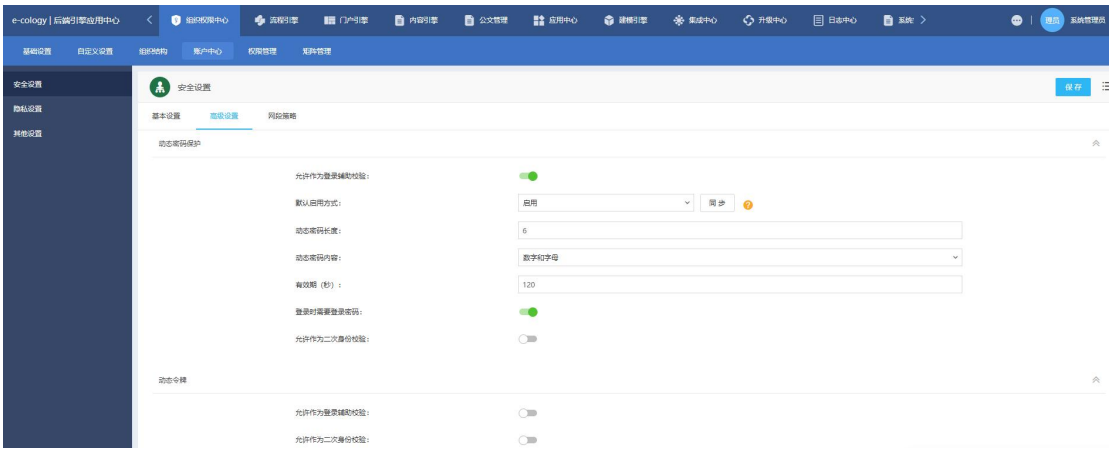
提醒：【弱密码禁止保存】选项早期版本可能没有，如果没有，可考虑升级 KB 补丁后启用。



如果有条件，上图中的【禁止在网段外登录】开关也可以打开，尤其是对超级管理员账号的限制。

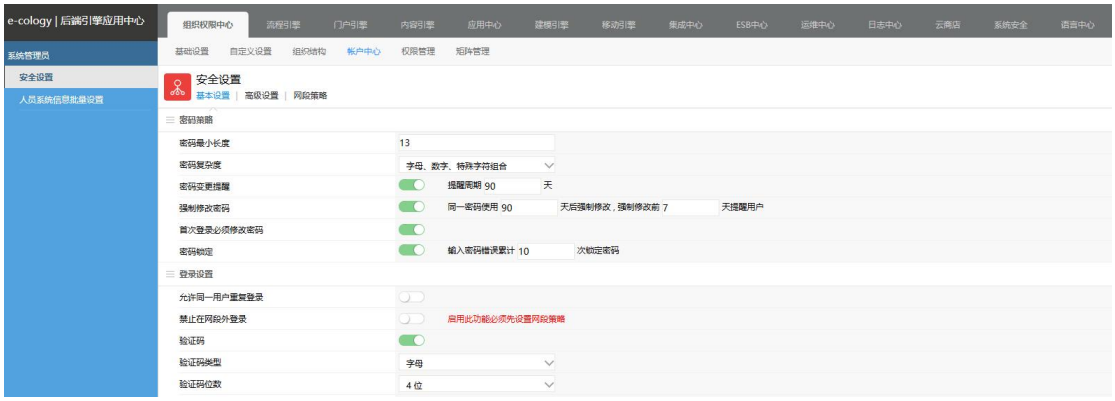
2、强烈建议启用动态密码等双因子认证机制

由于无论如何防范，都难以避免密码可能发生的泄露等风险。所以双因子是为了更好的保护密码泄露后造成的严重后果。**该项需要额外的硬件（比如短信设备、动态令牌等）支持，如有不清楚之处，可咨询您的专属客服或泛微对接人。**



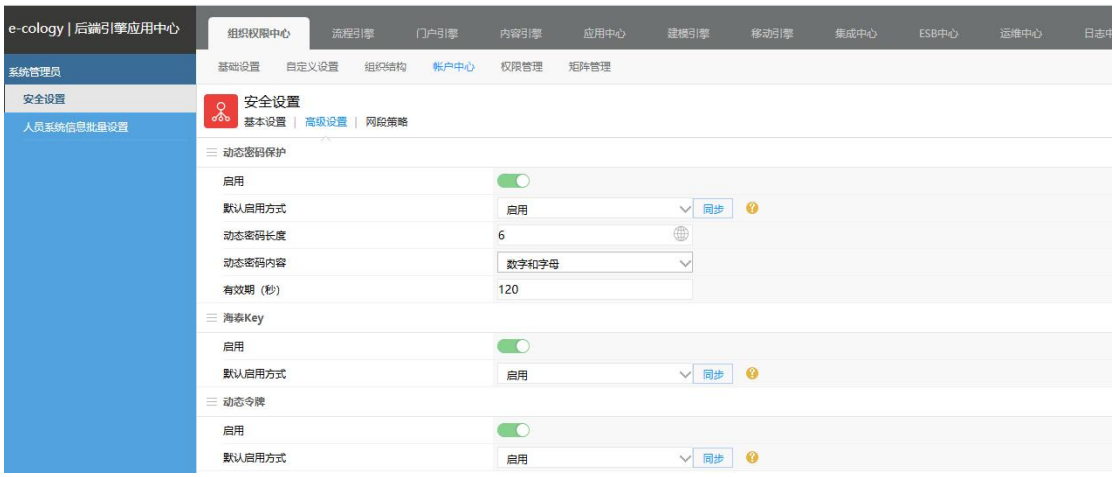
三、Ecology8.0 产品口令配置策略建议

1、建议按照下图中的方式配置系统口令复杂度：



2、强烈建议启用动态密码等双因子认证机制

由于无论如何防范，都难以避免密码可能发生的泄露等风险。所以双因子是为了更好的保护密码泄露后造成的严重后果。**该项需要额外的硬件（比如短信设备、动态令牌等）支持，如有不清楚之处，可咨询您的专属客服或泛微对接人。**

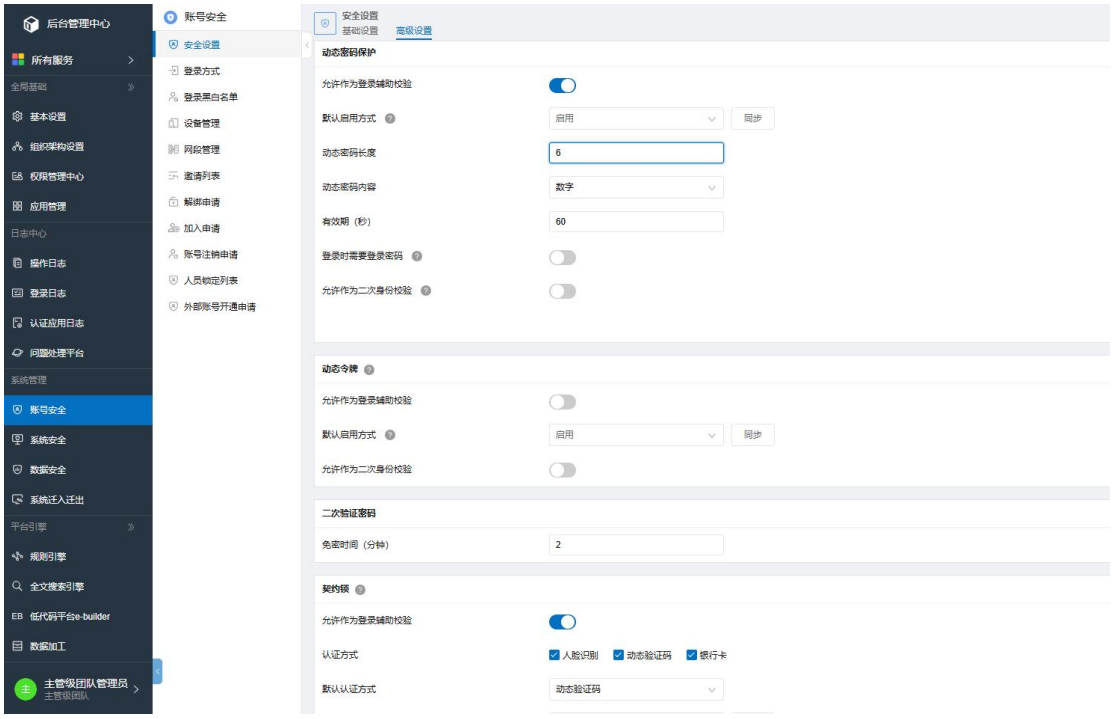


四、Ecology10.0 产品口令配置策略建议

1、建议按照下图中的方式配置系统口令复杂度：

2、强烈建议启用动态密码等双因子认证机制

由于无论如何防范，都难以避免密码可能发生的泄露等风险。所以双因子是为了更好的保护密码泄露后造成的严重后果。**该项需要额外的硬件（比如短信设备、动态令牌等）支持，如有不清楚之处，可咨询您的专属客服或泛微对接人。**



五、针对 sysadmin 账号启用 IP 白名单策略

由于 sysadmin 是泛微 ecology 产品的默认超级管理员账号，权限极大，容易成为攻击者的目标。因此，强烈建议针对该账号启用 IP 白名单策略。具体是通过网段策略来实现控制。

1、系统默认网段策略功能（Ecology8 和 Ecology9、ecology10 均具备相应的功能支持。

具体操作方式，可咨询您的专属客服或泛微对接人

2、安全补丁包提供的 sysadmin IP 白名单检测功能（ecology8/ecology9 支持）

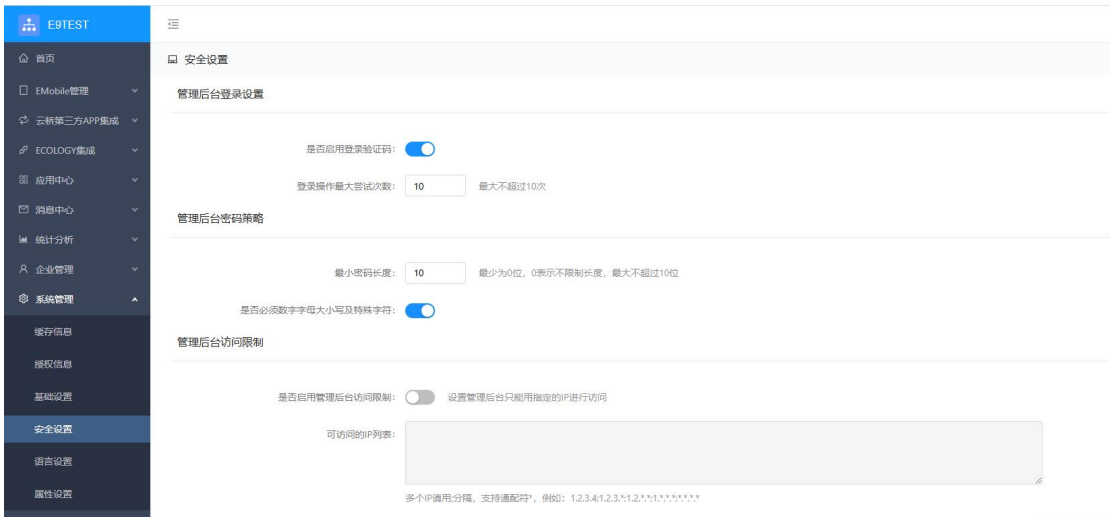
不同于 1 中的仅在登录时检测，本项功能是在运行时实时检测 sysadmin 管理员账号使用者的 IP 是否在白名单中，如果不在白名单，则会直接拒绝访问请求，并注销当前会话。

修改/ecology/WEB-INF/securityXML/weaver_security_custom_rules_1.xml，在下方添加如下代码（如果要放行某个网段，则填写 IP 的前半段即可，如 192.168.7. ，则代表 192.168.7.*都可以访问)：

```
<sysadmin-allow-login-ips>
<ip>192.168.7.200</ip>
<ip>192.168.10.</ip>
</sysadmin-allow-login-ips>
```

六、Emobile7 产品口令配置策略建议

1、建议按照下图中的方式配置系统口令复杂度



2、建议启用 EMobile7 管理后台使用的 IP 白名单策略

由于管理后台无需暴露给普通用户使用，因此，可以限制管理后台的使用 IP，避免互联网任意使用。