

档案软件 - 登录验证码功能【云丰档案软件功能介绍】

档案管理软件 · 安全管理功能介绍

光有账号密码还不够，登录时再加一道人机校验。云丰档案在登录环节提供验证码校验：输入密码后还需填写图片或短信验证码，确认是本人在操作，挡住机器自动批量尝试登录。

一、为什么需要登录验证码

自动化工具能不停地试账号密码，验证码就是把机器拦在门外：

机器撞库：脚本自动批量尝试登录，人工防不胜防；

密码泄露：密码一旦泄露，别人拿着就能直接登录；

登录无人拦：除了密码没有第二道验证，入口单薄；

异常无感：异地、异常登录没有额外确认。

登录验证码要在密码之外再确认一次人：机器过不来，异常多一道关。

二、怎么用

用户在登录页输入账号密码后，按提示完成验证码校验才能登录：

表1 登录验证码使用流程

环节	说明
输入凭证	用户输入账号与密码
触发校验	要求填写图片或短信验证码
人机确认	确认为本人或人工操作后放行
失败处理	验证码错误需重新获取再试
记录日志	登录成功与失败均记录

验证码在密码之外增加一道校验，常见形式有图形验证码、短信验证码。它有效拦截自动化批量登录，对异地或异常登录可叠加短信确认，进一步保护账号。

登录时叠加图形或短信验证码，确认是真人操作而非脚本自动尝试。验证码一次性有效，可与密码策略、锁定策略叠加，形成多重登录防护。

验证码一次性使用、过期即失效，可与密码策略、账号锁定叠加形成多重登录防护；对公共终端或外网访问，可强制要求验证码，内网可信环境则可按策略放宽。它以极低的使用成本挡住了大批量脚本自动尝试，使账号暴力破解难以规模化，是登录入口一道性价比很高的人机校验。

对疑似异常来源的登录可强制升级验证码强度，普通日常登录则保持顺畅，安全与体验按风险动态平衡。

对疑似异常来源升级校验强度，日常登录保持顺畅，安全与体验按风险平衡。

验证码失败次数过多同样触发限制，防止对验证码本身发起反复尝试。

验证码与账号密码双重校验同时进行，单独泄露其一都不足以登录，登录入口的安全门槛明显抬高。

三、核心能力

表2 核心能力一览

能力	一句话价值	关键细节
人机区分	挡脚本	验证码确认人工操作，拦截批量撞库。
二次校验	密码之外一道关	即使密码泄露，无验证码也难登录。
灵活形式	图文短信可选	支持图形或短信等多种验证码方式。
异常加强	可疑登录多验证	异常登录可叠加短信确认。
登录留痕	可审计	每次登录校验结果记入日志。

它挡住了大批量自动登录尝试，让账号暴力破解几乎不可能规模化。

四、典型使用场景

- 日常登录：全员登录时图形验证码挡自动化尝试；
- 异地登录：异地或非常用环境登录触发短信确认；
- 撞库防护：批量尝试被验证码和锁定策略一并拦截。

五、价值与产品定位

登录验证码在密码之外加了一道人机门槛：机器脚本批量试不过来，密码泄露也多一层保护。它是成本很低却很有效的登录防护手段，让档案系统的入口不再仅凭一道密码。它让每一次登录都确是本人在操作。

它与密码策略、账号锁定、统一认证共同构成登录安全链。云丰档案通过多重验证，把档案系统的登录入口守得更严，支撑敏感档案在信创环境下的安全访

问。云丰档案在登录入口加了一道人机校验。