## Windows 密码过滤组件 PasswordFiter - PwdFitr

### 1. 简介

PwdFitr 是 Windows 密码过滤 DLL，它可以在 Windows 中用户密码发生变化的前后通知外部程序。可用于将密码与外部数据库、目录服务或应用同步进行复制和同步。 pcns.bat 提供了密码通知的简单例子，它可以将用户更改后的密码写在一个文件中。

此密码过滤组件在 Windows 2012 X64 平台中测试通过。

### 2. 安全性

密码过滤组件过行在本系统帐户（Local System Account - LSA) 的安全上下文中，因此要保证 PwdFitr 和外部通知程序的安全性，避免被恶意替换造成密码的泄露。

### 3. 安装配置

1. 把生成的 pwdfitr.dll 复制到 C:\Windows\system32 目录
2. 修改注册表项 "HKLM->SYSTEM->CurrentControlSet->Control->Lsa->Notification Packages" 的值，添加 "pwdfitr" (无引号) 到名称列表中（新增加一行）
3. 修改注册表文件 pwdfitr.reg 中的各项参数以匹配实际场景和环境要求，然后双击此文件将其导入注册表，参数的详细说明见下节。

Windows Registry Editor Version 5.00

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\pwdfitr]

"logfile"=""

"maxlogsize"="8192"

"loglevel"="1"

"priority"="0"

"workingdir"="C:\\temp"

"urlencode"="true"

"output2log"="false"

"doublequote"="true"

"environment"=""

"preChangeProgWait"="7000"

"postChangeProgWait"="5000"

"postChangeProg"="c:\\program files\\pwdfitr\\pcns.bat"

"postChangeProgArgs"=""

"preChangeProg"=""

"preChangeProgArgs"=""

1. 在活动目录中确保密码复杂性安全策略被启用 "Domain Security Policy\Windows Settings\Security Settings\Account Policies\Password Policy\Passwords must meet complexity requirements"
2. 重新启动服务器
3. 以上操作需要在每台域控制器 (Domain Controller) 中都要进行一次，只读域控制器 (RODC) 除外。

### 4. 注册表配置参数

注册表中所有参数的类型将为字符型 (REG\_SZ)，可以参见 pwdfitr.reg .

注册表中的参数名称和作用如下所示：

1. **preChangeProg**

预更改程序，在用户更改密码前执行的程序，如果外部程序（或脚本）返回一个非 0 值，则用户的密码更改操作将被拒绝，利用此程序可以对用户的密码更改操作进行事先控制和各种检查。

如果外部程序为脚本程序，由此值不能直接是脚本程序的名称，而应该是脚本程序的解释器对应的可执行文件，如 perl.exe 或 powershell.exe 等。

如果此参数为空，则密码过滤组件将不在此环节获取用户密码。

1. **preChangeProgArgs**

预更改程序 preChangeProg 的参数，如果为空，则密码过滤组件在调用外部程序时，将只传递两个参数，即用户名和密码。

这个参数一般用于特定平台和脚本程序，假设当预更改程序 Java 时，则 preChangeProg 参数的值为 "C:\Program Files\Java\bin\jre.exe", preChangeProgArgs 参数的值就是实际要传给 Java 过行时的任何参数以及要过行处理密码的类，如 MyJavaClasses 等，这样最后密码过滤组件调用和执行的应用程序应是：

*"C:\Program Files\Java\bin\jre.exe" -cp "C:\Program Files\MyJavaClasses" username password*

注意： preChangeProg 参数必须为可执行程序，且不能带参数。

1. **preChangeProgWait**

预更改程序 preChangeProg 的最长执行时间（单位：毫秒），设置此值以防止预处理程序时间过长造成用户更改密码操作都无法进行。

1. **postChangeProg**

后更改程序，在用户更改密码操作完成后被调用，其规则与预更改程序类似（只能为可执行程序，且无参数）

1. **postChangeProgArgs**

后更改程序 postChangeProg 的参数，类似于 preChangeProgArgs。

1. **postChangeProgWait**

后更改程序 preChangeProg 的最长执行时间（单位：毫秒），设置此值以防止预处理程序时间过长造成用户更改密码操作都无法进行。

注：只有postChangeProg执行完成后，Windows才会把密码更改结果才反馈给用户。

1. **logfile**

包含路径日志文件，如无将被创建。

1. **loglevel**

日志级别，范围为 0-3, 分别代表： 0 - 禁止日志, 1 - 记录错误, 2 - 记录调试信息, 3 - 记录包括密码在的内全部设计信息（不推荐），日志级别大于0时，一定要指定日志文件。

1. **maxlogsize**

指定日志文件最大字节数（单位KB），当日志文件到达此大小时，最早的日志将被截断只保留最新 25%，旧的日志文件将被重命名 .bak。 当此值为 0 将禁用文件大小检查和日志截断。

1. **urlencode**

对于密码是否使用 URL 编码，必须为 "true" 或 "false"，建议为 true 以防止复杂密码（包含空格、引号等）在向外部程序传递时出现错误。

1. **doublequote**

对于密码是否使用双引号括起来。必须为 "true" 或 "false"，在引号内的密码中如果也包含引号，将被替换为 \"，除非 urlencode 设置为 true，当 urlencode 设置为 true 时，已没必要将密码使用引号括起来。

1. **output2log**

是否记录外部应用程序的输出内容，必须为 "true" 或 "false"，一般为 false

1. **priority**

调用外部应用程序的优先级，优先级，-1 低，0 正常，1 高，建议默认值 0。

1. **workingdir**

密码过滤组件及被调用外部应用程序的默认工作目录。

1. **environment**

被调用外部应用程序的环境块（环境变量），如果未使用，保留为空。