新建1个 user组的账户，1个administrators 组的账户

关闭 uac ，并重启机器，[参考](http://www.xitongcheng.com/jiaocheng/win7_article_35485.html)

新建一个程序（AdminApp1.exe），其能读写注册表 （需要admin权限）

新建一个程序（AdminForm.exe），其用来启动第一个程序

核心代码

try

{

Process MBRTProcess = new Process();

MBRTProcess.StartInfo.UserName = "user-a";

string strPWD = "1111@aaaa";

SecureString password = new SecureString();

foreach (char c in strPWD.ToCharArray())

{

password.AppendChar(c);

}

MBRTProcess.StartInfo.Password = password;

MBRTProcess.StartInfo.WorkingDirectory = AppDomain.CurrentDomain.BaseDirectory;

MBRTProcess.StartInfo.FileName = "AdminApp1.exe";

MBRTProcess.StartInfo.Arguments = "/run /wu";

MBRTProcess.StartInfo.UseShellExecute = false;

MBRTProcess.Start();

}

catch (Exception error)

{

MessageBox.Show(error.Message);

}

其中需要指定 有administrators 权限的 用户名 ，密码 以及要启动的程序

启动后 AdminApp1.exe 具有了 管理员权限

遗留问题： 需要整理文档， 实验xp 能否执行， win10能否执行

3个关闭uac 的注册表，真正其作用的是哪个，需要确定

参考文章：

<https://blog.csdn.net/woshinia/article/details/7850295>

http://blog.sina.com.cn/s/blog\_457b98580100az02.html