

史上最全九种破解Xp登录密码方法 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/454/2021\\_2022\\_\\_E5\\_8F\\_B2\\_E4\\_B8\\_8A\\_E6\\_9C\\_80\\_E5\\_c100\\_454449.htm](https://www.100test.com/kao_ti2020/454/2021_2022__E5_8F_B2_E4_B8_8A_E6_9C_80_E5_c100_454449.htm)

Windows XP的使用过程中如果你是一个很容易遗忘的人，那么一定不要忘记在第一次设置密码的同时创建一张可以恢复Windows XP中的账户密码的启动盘，它可以让你免去格式化硬盘的烦恼。从“控制面板”中找到“用户账户”项，选中自己的账户进入如图所示的控制界面，我们可以看到左侧任务列表中有一项“阻止一个已忘记的密码”，点击后便可打开“忘记密码向导”，向导会提示插入一张格式化过的空白磁盘，操作过程中会让你输入该账户所使用的密码，很快便可以创建一张密码重设盘。以后，当我们忘记了账户密码的时候，在没有使用“欢迎屏幕”登录方式的情况下登录到Windows XP后，按下“Ctrl Alt Del”组合键，出现“Windows 安全”窗口，点击选项中“更改密码”按钮，出现更改密码窗口。这个窗口中，将当前用户的密码备份，点击左下角“备份”按钮，激活“忘记密码向导”，按照提示创建密码重设盘。如果在Windows XP的登录窗口输入了错误的密码，就会弹出“登录失败”窗口，如果你的确想不起来自己的密码是什么时，可点击“重设”按钮，启动密码重设向导，通过刚才所创建的密码重设盘，就可以用这张密码重设盘更改密码并启动系统。重新设定密码，登录Windows XP。“密码重设盘”的创建，含有一定的危险性，因为任何人都可以使用这一张“密码重设盘”来登录Windows XP，都可以以该用户的名义进入用户帐户，操作真正用户所能操作的一切，所以必须将“密码

重设盘”保存在适当的地方，以防丢失或失泄密。方法1利用“administrator”（此方法适用于管理员用户名不是“administrator”的情况）我们知道在安装Windows XP过程中，首先是以“administrator”默认登录，然后会要求创建一个新账户，以进入Windows XP时使用此新建账户登录，而且在Windows XP的登录界面中也只会出现创建的这个用户账号，不会出现“administrator”，但实际上该“administrator”账号还是存在的，并且密码为空。当我们了解了这一点以后，假如忘记了登录密码的话，在登录界面上，按住Ctrl Alt键，再按住Del键二次，即可出现经典的登录画面，此时在用户名处键入“administrator”，密码为空进入，然后再修改“zhangbp”的口令即可。方法2删除SAM文件（注意，此法只适用于WIN2000）Windows NT/2000/XP中对用户帐户的安全管理使用了安全帐号管理器（Security Account Manager，SAM）的机制，安全帐号管理器对帐号的管理是通过安全标识进行的，安全标识在帐号创建时就同时创建，一旦帐号被删除，安全标识也同时被删。安全标识是唯一的，即使是相同的用户名，在每次创建时获得的安全标识完全不同。因此，一旦某个帐号被用户名重建帐号，也会被赋予不同的安全标识，不会保留原来的权限。安全帐号管理器的具体表现就是%SystemRoot%\system32\config\sam文件。SAM文件是Windows NT/2000/XP的用户帐户数据库，所有用户的登录名以及口令等相关信息都会保存在这个文件中。知道了这些，我们的解决办法也产生了：删除SAM文件，启动系统，它会重建一个干净清白的SAM，里面自然没有密码了。不过，这么简单的方法在XP是不适用的，可能微软以此为BUG，做了限制……

所以现在在XP系统下，即使你删除了SAM，还是不能删除密码，反而会使系统启动初始化出错，从而进入死循环而不能进系统！！方法3从SAM文件中找密码（前提.....会使用DOS基本命令就行）在系统启动前，插入启动盘，进入：  
C：WINNTSystem3Config用COPY命令将SAM文件复制到软盘上。拿到另一台机子读取。这里需要的工具是LC4，运行LC4，打开并新建一个任务，然后依次击“IMPORT Import from SAM file”，打开已待破解的SAM文件，此时LC4会自动分析此文件，并显示出文件中的用户名；之后点击“Session Begin Audit”，即可开始破解密码。如果密码不是很复杂的话，很短的时间内就会得到结果。不过，如果密码比较复杂的话，需要时间会很长，这时我们就需要用下面的方法了。方法4用其他SAM文件覆盖（前提是你可以得到另外一台电脑的SAM文件和它的密码.....个人觉得是最为可行的办法）1如上所说，SAM文件保存着登录名以及口令，那么我们只要替换SAM文件就是替换登录名以及口令了。不过，这个替换用的SAM文件的“产地”硬盘分区格式要和你的系统一样（看是FAT32还是NTFS，你自己确认）。最好这个“产地”的系统没有设密码，安全方面设置没动过（实际上很大部分的个人电脑都是这样），当然，比较保险的方式是把XP的[Win NTSystem 32Config]下的所有文件覆盖到[C：Win NTSystem 32Config]目录中（假设你的XP安装在默认分区C：），2如果得不到别人的帮助（我是说“万一”），你可以在别的分区上在安装一个XP系统，硬盘分区格式要和原来的一样，并且请你注意一定不要和原来的XP安装在同一分区！在开始之前，一定要事先备份引导区MBR，备份MBR的

方法有很多，使用工具软件，如杀毒软件KV3000等。装完后用Administrator登陆，现在你对原来的XP就有绝对的写权限了，你可以把原来的SAM考下来，用10PHTCRACK得到原来的密码。也可以把新安装的XP的Win NTSystem 32Config下的所有文件覆盖到C：Win NTSystem 32Config目录中（架设原来的XP安装在这里），然后用KV3000恢复以前悲愤的主引导区MBR，现在你就可以用Administrator身份登陆XP了。[2号方案我自己都觉得麻烦，还是1号：叫别人帮忙比较好.....]

「另外，据说C：windows epair 目录下的SAM是原始版本的，可以用它来覆盖 system32下的这个 SAM，这样就可以删除现在的密码，而恢复到刚开始安装系统时的密码了。如果这个密码为空，岂不是.....」 100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)