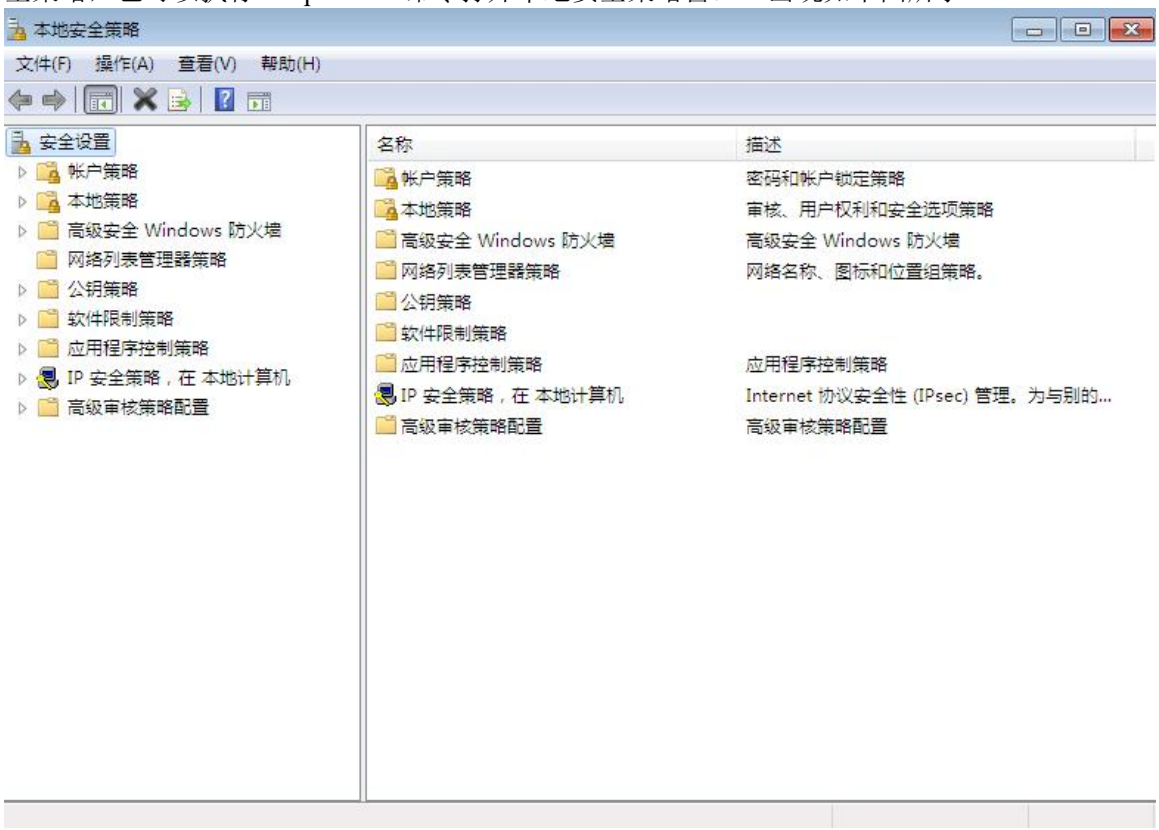
一、本地安全策略概述

本地安全策略影响本地计算机的安全设置，当用户登录到某台 windows7 计算机上时，就会受到此台计算机的本地安全策略的影响！

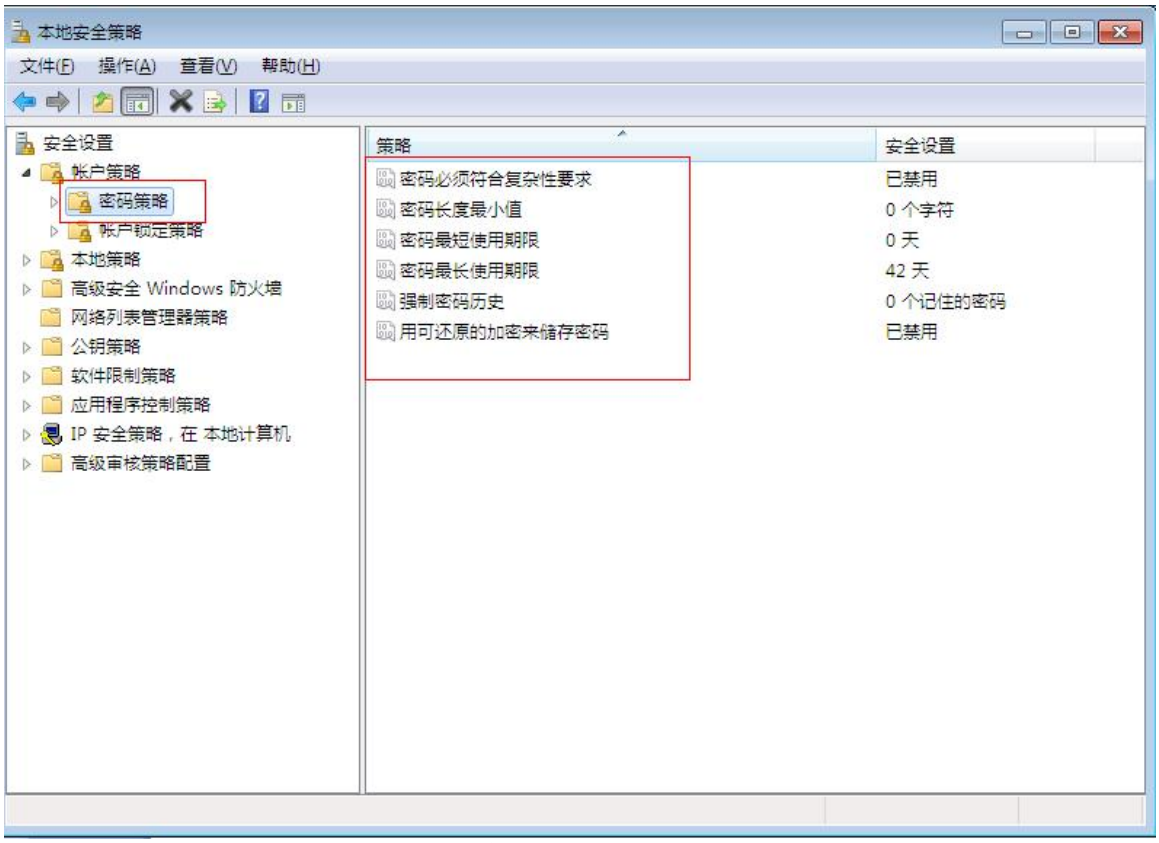
要管理本地安全策略，可以单击“开始”菜单-控制面板-系统和安全-管理工具，然后双击”本地安全策略，也可以执行“secpol.msc"命令打开本地安全策略窗口！出现如下图所示



一、/账户策略

账户策略主要分为两个部分：密码策略和账户锁定策略

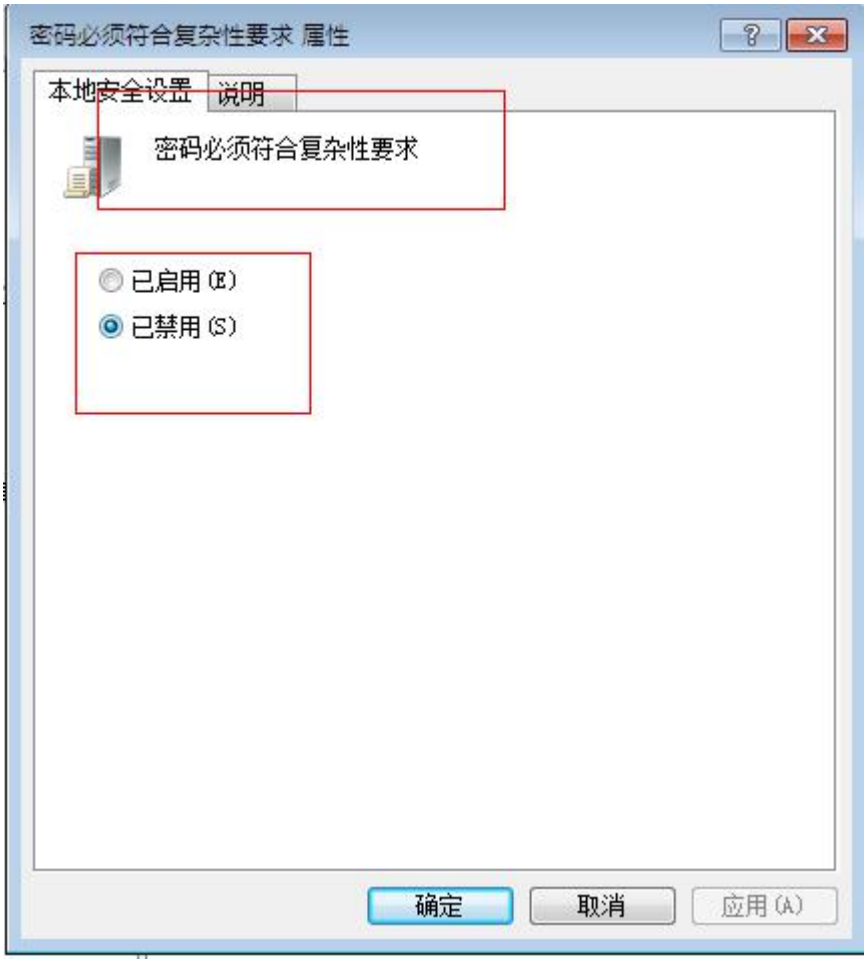
1、密码策略主要包括以下几个具体策略



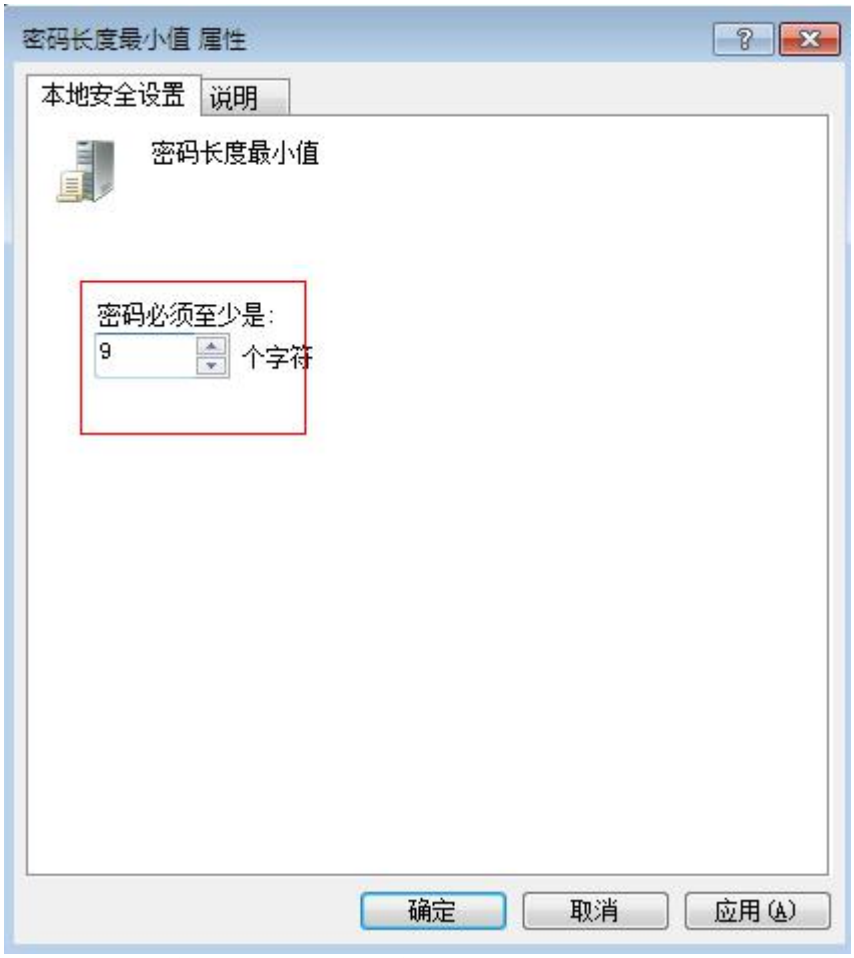
现在就来一一讲下各个密码策略的设置意义！

- 密码必须符合复杂性要求：启用此策略后，用户账户使用的密码必须符合复杂性的要求。密码复杂性是指密码中必须包含以下四类字符中的三类字符。
- 英文大写字母（A 到 Z）
- 英文小写字母（a 到 z）
- 10 个基本数字（0 到 9）
- 特殊符号（例如!、@、$、#）

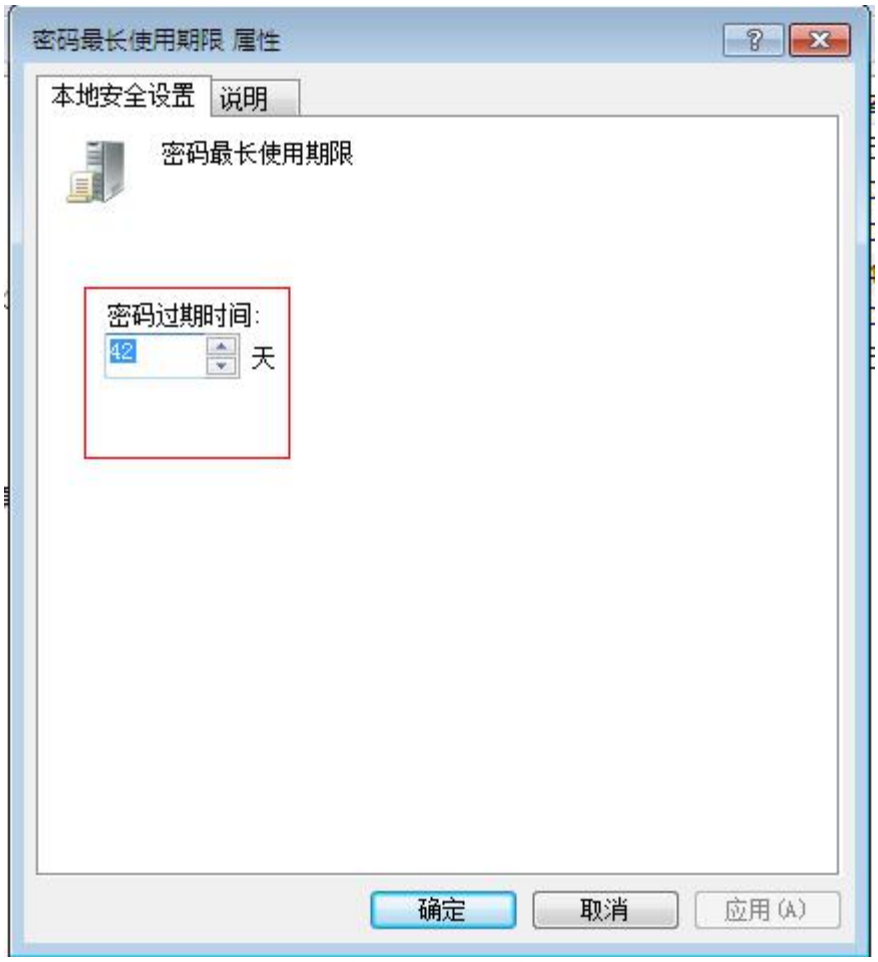
双击该策略后的设置对话框如下图显示!



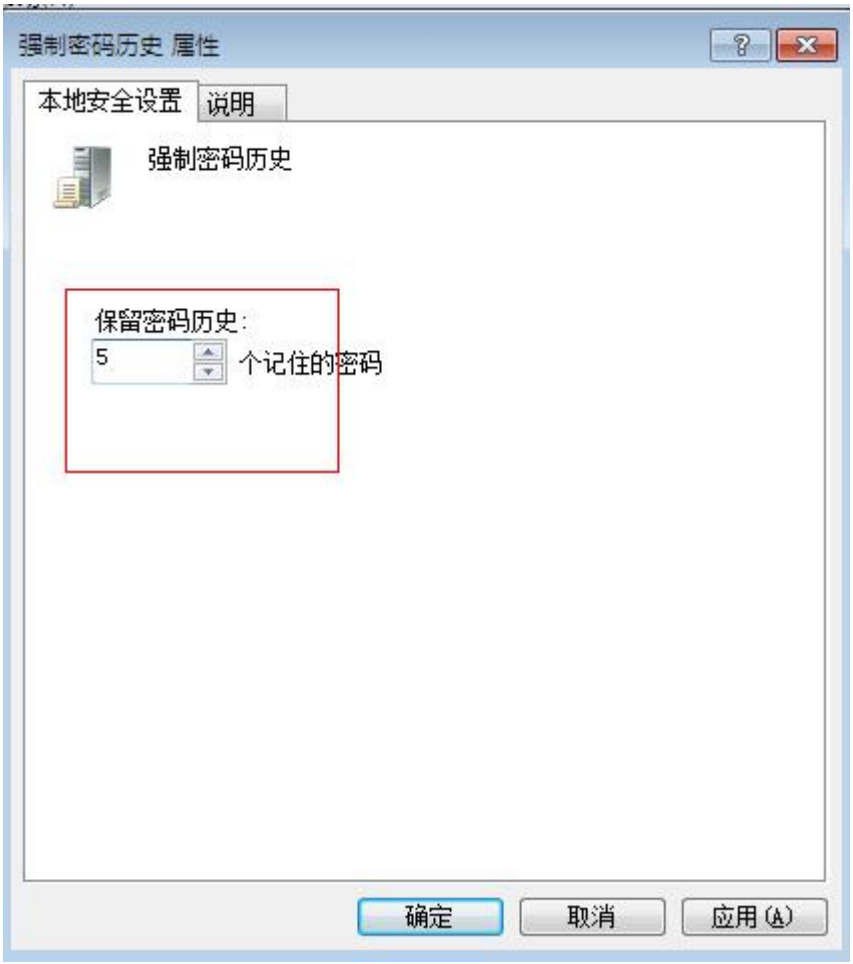
- 密码长度最小值：该项安全设置确定用户账户的密码包含的最少字符个数。设置范围 0~14，将字符数设置为 0，表示不要求密码。双击该策略后的设置对话框如下图所示：



- 密码最长使用期限：指密码使用的最长时间：单位为天。设置范围 0~999，默认设置时 42 天，如果设置为 0 天，表示密码用不过期。双击该策略后的设置对话框如下图所示



- 密码最短使用期限：此安全设置确定在用户更改某个密码之前至少使用该密码的天数。可以设置一个介于 1 和 998 天之间的值，或者将天数设置为 0，表示可以随时更改密码，密码最短使用期限必须小于密码最长使用期限，除非密码最长使用期限为 0.如果密码最长使用期限设置为 0，那么密码最短使用期限可以设置为 0 到 998 之间的任意值！
- 强制密码历史：指多少个最近使用过的密码不允许再使用。设置范围在 0~24 之间，默认值为 0 ，代表可以随意使用过去使用的密码，双击该策略后的设置对话框如图所示

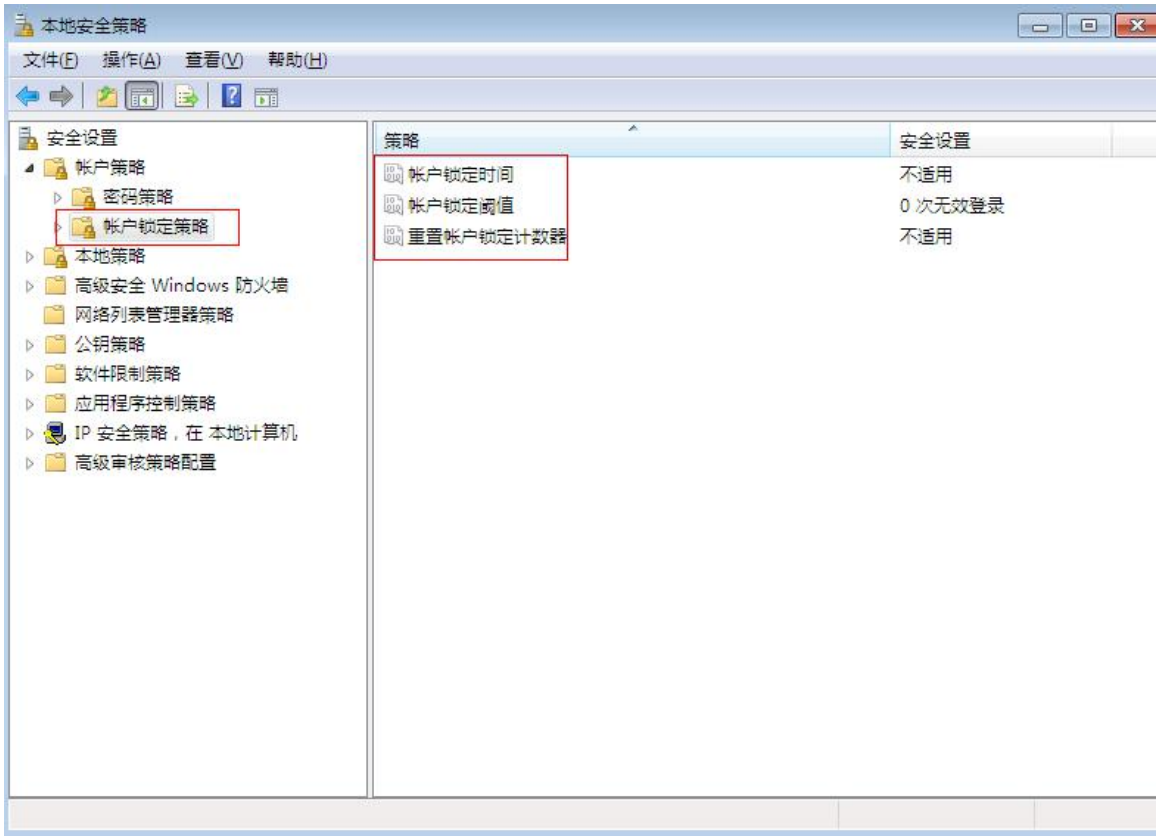


- 用可还原的加密来出储存密码：指密码的存储方式，是否用可以还原的加密方式存储，默认情况下，存储的密码只有操作系统能够访问，如果某些应用程序需要直接访问某个账户的密码，则必须将此策略启用，此策略的应用会使安全性降低，所以一般不启用！

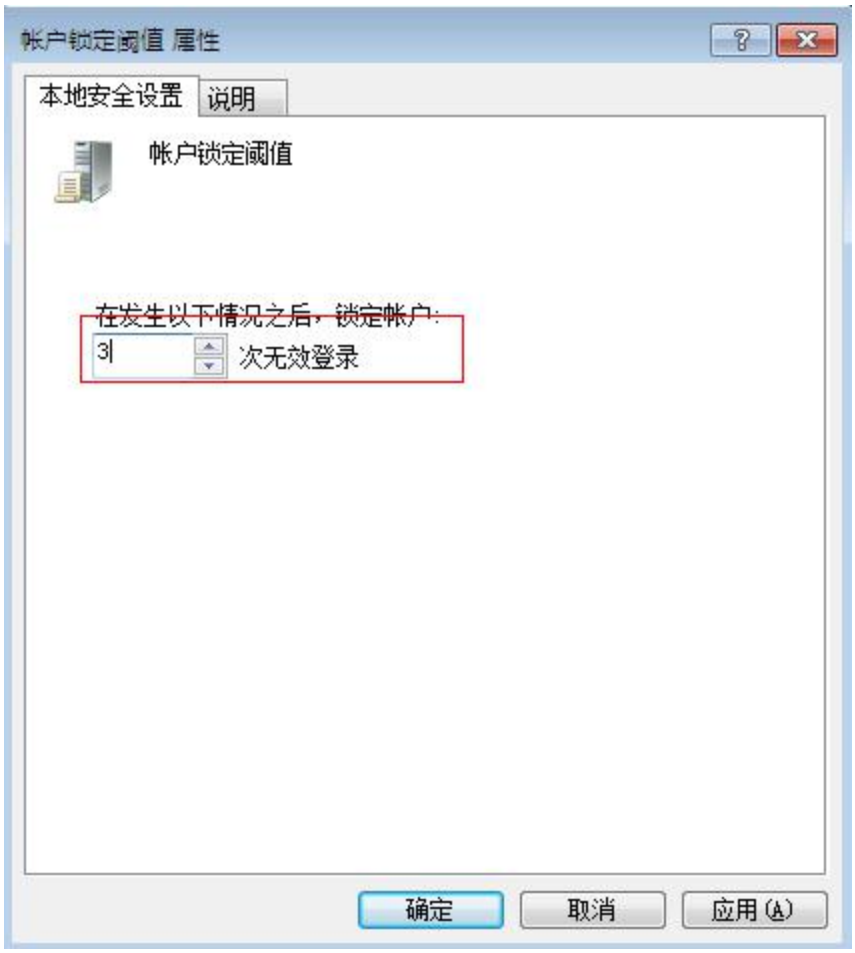
二、账户锁定策略

账户锁定策略是指当用户输入错误密码的次数达到一个设定值时，就将此账户锁定，锁定的账户暂时不能登录，只有等超过指定时间自动解除锁定或由管理员手动解除锁定

账户锁定策略包括以下三个设置：



- 账户锁定阈值：指用户输入几次错误的密码后，将用户账户锁定。设置范围为 0~999.如图，默认值为 0，代表不锁定账户，对于用户使用 ctrl+alt+del 或带有密码保护的屏幕保护程序锁定的工作站或成员服务器，失败的密码尝试将计入失败的登录尝试次数中



- 账户锁定时间：指当用户账户被锁定后，多长时间后自动解锁，单位为分钟，设置单位为 0~99999,0 代表必须有管理员手动解锁
- 重置账户锁定计数器：指用户输入密码错误开始计数时，计数器保持的时间，当该时间过后，计数器将重置为 0，如果定义了账户锁定阈值，则该重置时间必须小于或等于账户锁定时间

注意啦：账户锁定策略对本地管理员账户 Administrator 无效