密码策略：

|  |  |  |  |
| --- | --- | --- | --- |
| 策略编号 | 策略名称 | 参数值（默认值） | 说明 |
| 11010101 | 密码必须符合复杂性要求 | 1（开启） | 确定密码是否必须符合复杂性要求。  启用此策略，密码必须符合下列最低要求:  1、不能包含用户的帐户名，不能包含用户姓名中超过两个连续字符的部分；  2、至少有六个字符长；  3、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) * 非字母字符(例如 !、$、#、%) |
| 11010102 | 最短密码长度 | 6 | 确定用户帐户密码包含的最少字符数。  可以将值设置为介于 1 和 32 个字符之间，  或者将字符数设置为 0 以确定不需要密码。 |
| 11010201 | 密码最短使用期限 | 0 | 确定在用户更改某个密码之前必须使用该密码一段时间(以天为单位)。  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，允许立即更改密码。   * 密码最短使用期限必须小于密码最长使用期限，除非将密码最长使用期限设置为 0，指明密码永不过期。 * 如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为介于 0 和 998 之间的任何值。 * 如果希望“强制密码历史（个数）”有效，则需要将密码最短使用期限设置为大于 0 的值。 * 如果没有设置密码最短使用期限，用户则可以循环选择密码，直到获得期望的旧密码。 * 默认设置没有遵从此建议，以便管理员能够为用户指定密码，然后要求用户在登录时更改管理员定义的密码。 * 如果将密码历史设置为 0，用户将不必选择新密码。因此，默认情况下将“强制密码历史（个数）””设置为 1。 |
| 11010202 | 密码最长使用期限 | 60 | 确定在系统要求用户更改某个密码之前可以使用该密码的期间(以天为单位)。可以将密码设置为在某些天数(介于 1 到 999 之间)后到期，或者将天数设置为 0，指定密码永不过期。如果密码最长使用期限介于 1 和 999 天之间，密码最短使用期限必须小于密码最长使用期限。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为介于 0 和 998 天之间的任何值。  注意:  安全最佳操作是将密码设置为 30 到 90 天后过期，具体取决于您的环境。这样，攻击者用来破解用户密码以及访问网络资源的时间将受到限制。 |
| 11010203 | 提示用户在密码过期之前进行更改 | 7 | 确定提前多长时间(以天为单位)向用户发出其密码即将过期的警告。  借助该提前警告，用户有时间构造足够强大的密码。 |
| 11010301 | 强制密码历史（个数） | 24 | 确定再次使用某个旧密码之前必须与某个用户帐户关联的唯一新密码数。  该值必须介于 0 个和 24 个密码之间。  此策略使管理员能够通过确保旧密码不被连续重新使用来增强安全性。 |
| 11010302 | 强制密码历史（天数） | 15 | 确定再次使用某个旧密码之前必须与某个用户帐户关联的唯一新密码天数。  安全最佳操作是设置为 10 到 30 天 |
| 11010401 | 用可还原的加密来储存密码 | 0（关闭） | 使用此安全设置确定系统是否使用可还原的加密来储存密码。  只针对账户密码有效。其他部分另外定义 |
| 11010501 | 新用户默认密码 | User,Pwd,123 | 新增加用户的默认密码。  管理员在增加用户时没有指定用户密码，则使用该默认密码。 |

交互式登录：

|  |  |  |  |
| --- | --- | --- | --- |
| 策略编号 | 策略名称 | 参数值（默认值） | 说明 |
| 11020101 | 显示最后登录用户 | 0（禁用） | 确定是否在 UMP 登录屏幕中显示最后登录到系统的用户账号。  如果启用该策略，则会在登录屏幕中显示最后成功登录的用户账号。  如果禁用该策略，则不会显示最后登录的用户账号。 |
| 11020102 | 允许记住用户账号和密码 | 0（禁用） | 确定是否允许在客户端机器上保存用户账号和登录密码。  只有 开启“显示最后登录用户”才能配置该选项 |
| 11020103 | 允许LDAP账户自动登录 | 0（禁用） | 确定是否允许LDAP账户自动登录UMP系统。  LDAP账户必须已经导入或同步到UMP系统中。  当前登录windows系统的用户必须是域验证登录。 |
| 11020104 | 登录后提示信息文本 | 无 | 用户成功登录后，显示的WELCOME的内容。  如果值为“无”，登录系统后没任何提示信息。 |
| 11020105 | 新用户登录后强制修改密码 | 1（开启） | 新用户登录UMP系统后必须修改创建该用户时设置的密码。 |
| 11020201 | 超过登录时间后强制注销 | 0（禁用） | 启用此策略时，一旦客户端的登录时间过期，该策略便会强制断开与 UMP 服务器建立的客户端会话。该值范围为 1 – 16（小时）  如果禁用此策略，即便在客户端登录时间过期后，仍允许维持已建立的客户端会话。  0表示禁用此策略 |
| 11020202 | 无操作强制注销 | 0（禁用） | 启用此策略是，一旦客户端在指定的分钟内没有键盘、鼠标等操作，该策略便会强制断开与UMP服务器建立的会话。该值范围为 1 – 60（分钟） |
| 11020301 | 允许同一账户打开多个UMP系统 | 0（禁用） | 启用此策略指同一账号在同一时间内只能登录进入一个UMP系统实例。 |
| 11020302 | 同一计算机尝试登录次数 | 5 | 启用此策略指，在同一台计算机尝试登录UMP的次数。超过该次数后，30分钟后重新计数。此数值必须 >= 登录账户锁定策略中的“锁定阈值”  0表示禁用此策略。 |
| 11020401 | 重命名系统超级管理员帐户 | Administrator | 此设置确定是否存在另一个帐户 \*\*\* 与帐户 Administrator 的安全标识符(UID)相关联。因为人们都知道重命名 Administrator 帐户会使未授权的人猜测此权限用户名和密码组合的难度稍微大一些。 |

锁定策略：

|  |  |  |  |
| --- | --- | --- | --- |
| 策略编号 | 策略名称 | 参数值（默认值） | 说明 |
| 11030101 | 帐户锁定阈值 | 0 | 此设置确定导致用户帐户被锁定的登录尝试失败的次数。  在管理员重置锁定帐户或帐户锁定时间期满之前，无法使用该锁定帐户。  可以将登录尝试失败次数设置为介于 0 和 10之间的值。  如果将值设置为 0，则永远不会锁定帐户。 |
| 11030102 | 帐户锁定时间 | 无 | 此设置确定锁定帐户在自动解锁之前保持锁定的分钟数。  可用范围从 0 到 1440分钟。  如果将帐户锁定时间设置为 0，帐户将一直被锁定直到管理员明确解除对它的锁定。  如果定义了帐户锁定阈值，则帐户锁定时间必须 >= 重置时间。  默认值: 无，因为只有在指定了帐户锁定阈值时，此设置才有意义。 |
| 11030103 | 在此后复位帐户锁定计数器 | 无 | 此设置确定在某次登录尝试失败之后将登录尝试失败计数器重置为 0 次错误登录尝试之前需要的时间。可用范围是 1 到 1440 分钟。  如果定义了帐户锁定阈值，此重置时间必须小于或等于帐户锁定时间。  默认值: 无，因为只有在指定了帐户锁定阈值时，此设置才有意义。 |