

说明

因为CIS Benchamrk中的条目太多，所以有必要单开一页来记录。Benchmark的基准OS版本是Windows 11 23H2，而我的VMware中的虚拟机服务器则是Window Server 2022. 共有19章节，一一列举如下。

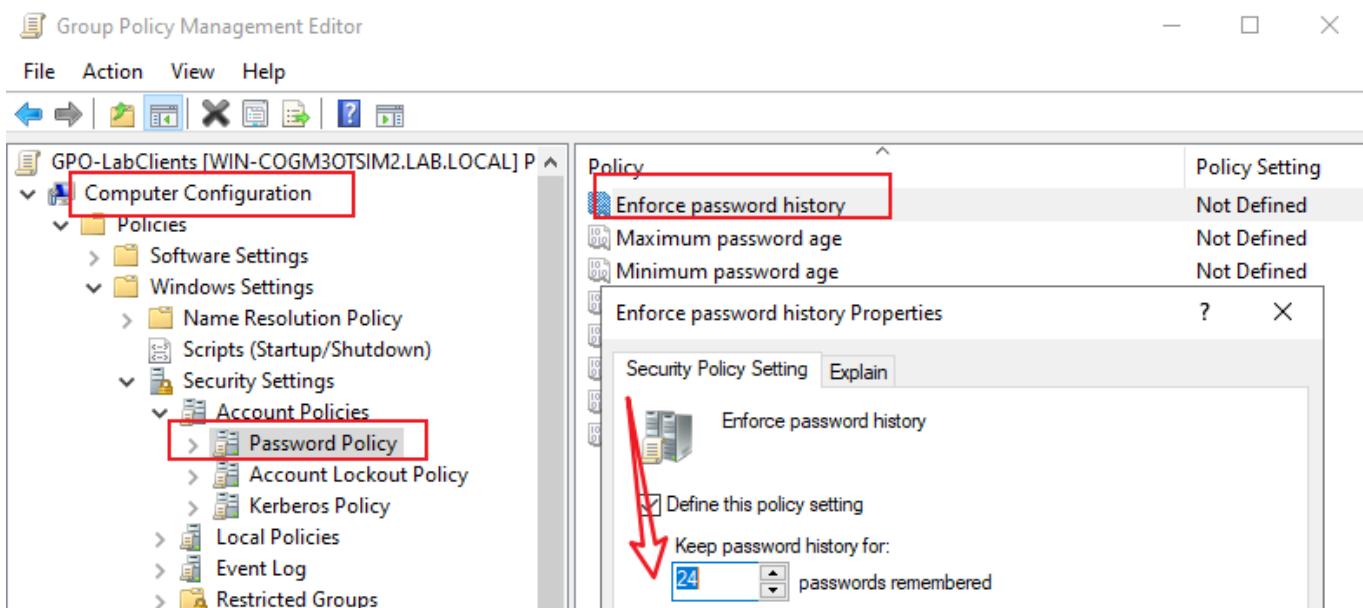
1.Account Policies

1.1 Password Policy

1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)

微软对于Win11系统的最长密码记录就是24世代。当用户长时间使用同一密码，攻击者使用暴力破解获取密码的可能性就越大。如果公司要求员工定期进行密码更换，但却未禁止用户复用密码，则定期变更密码的效果会大打折扣。而且用户会倾向于设置新密码为增量形式，比如password01,password02,易记但容易被猜到。设置方法

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history



1.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'

这个用于设置每一个密码可以用多久。如果设置为0，则密码永不过期。在1.1 Password Policy的设置和1.2 Account Lockout Policy的设置必须在**Default Domain Policy**中的GPO里修改，以对全Domain生效。如果是在其他GPO里修改，则只影响该GPO对应的用户账户或计算机。当然，添加其他Password Policy到特定用户或用户组也是OK的，一般是通过Active Directory Administrative Center. 参考期限60Days



目前美国NIST已经提倡不需要定期修改密码，而是应该提高密码的复杂度以降低被攻破的风险。现在的最佳实践(Best Practice)是只在确认密码已泄露的情况下，强制要求用户修改密码。

设置方法

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays the GPO structure: GPO-LabClients [WIN-COGM3OTSIM2.LAB.LOCAL] > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy. The 'Maximum password age' policy is selected in the main pane. The right pane shows the 'Maximum password age Properties' dialog. It includes a 'Security Policy Setting' section with a checkbox labeled 'Define this policy setting' and a field 'Password will expire in:' containing '999 days'. A red arrow points from the text 'Max的设置' to the '999 days' field. Below the dialog, a note states '范围是1-999天 Mix的设置范围是0-998天'.

1.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)'

同上，设置的是最小值，默认是1天。

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays a GPO named 'GPO-LabClients [WIN-COGM3OTSIM2.LAB.LOCAL]' under 'Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy'. On the right, the 'Policy' pane lists three policies: 'Enforce password history', 'Maximum password age', and 'Minimum password age'. The 'Minimum password age' policy is selected, opening its properties window titled 'Minimum password age Properties'. The 'Security Policy Setting' tab is active. It shows the 'Minimum password age' icon and a checked checkbox labeled 'Define this policy setting'. Below it, a field labeled 'Password can be changed after:' contains the value '998' with a dropdown arrow next to it, indicating days.

设置方法

From:

<https://trident365.com/> - 三叉戟

Permanent link:

https://trident365.com/doku.php?id=resources:os:windows_11:baseline&rev=1731853272

Last update: **2024/11/17 23:21**

