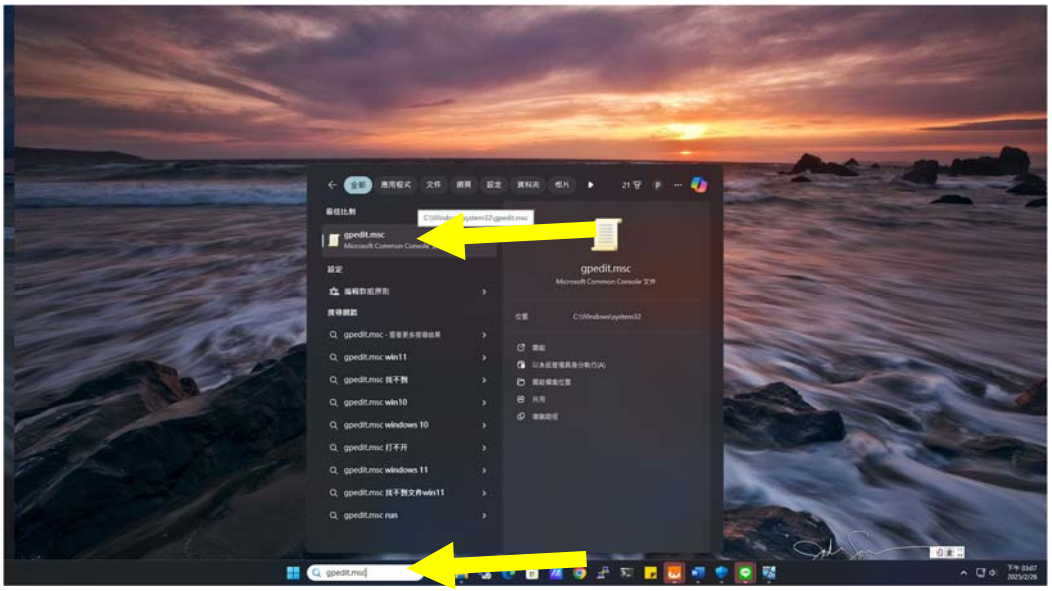
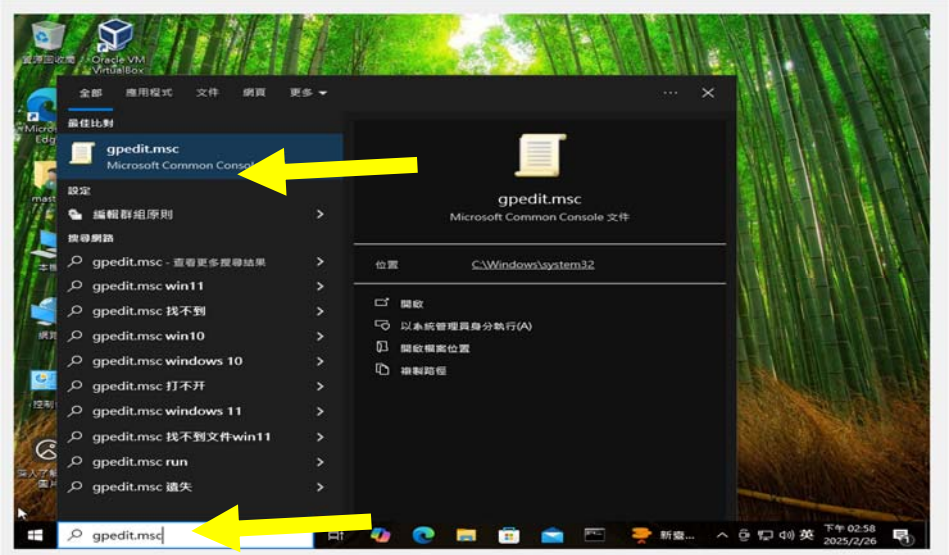
個人電腦登入密碼原則修方法

一、開始 -> 搜尋 -> 輸入　Gpedit.msc
　　上方會出現搜尋結果-> 左 KEY 執行

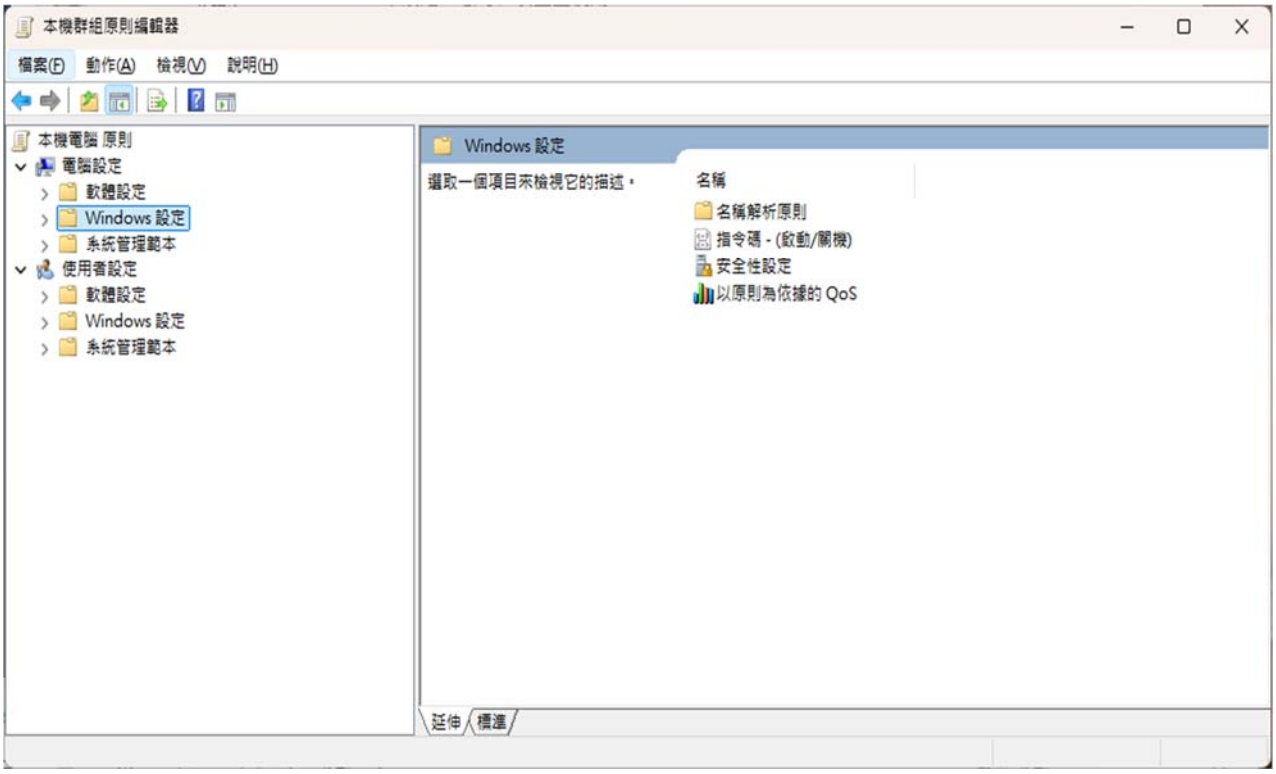
Windows 11　<搜尋在工具列中央>



Windows 10　<搜尋在工具列左側>



進入電腦設定視窗


本機群組原則編輯器
檔案(F) 動作(A) 檢視(V) 說明(H)
本機電腦 原則
電腦設定
軟體設定
Windows 設定
系統管理範本
使用者設定
軟體設定
Windows 設定
系統管理範本
Windows 設定
選取一個項目來檢視它的描述。
名稱
名稱解析原則
指令碼 - (啟動/關機)
安全性設定
以原則為依據的 QoS
延伸
標準

二、左側功能表 逐層展開

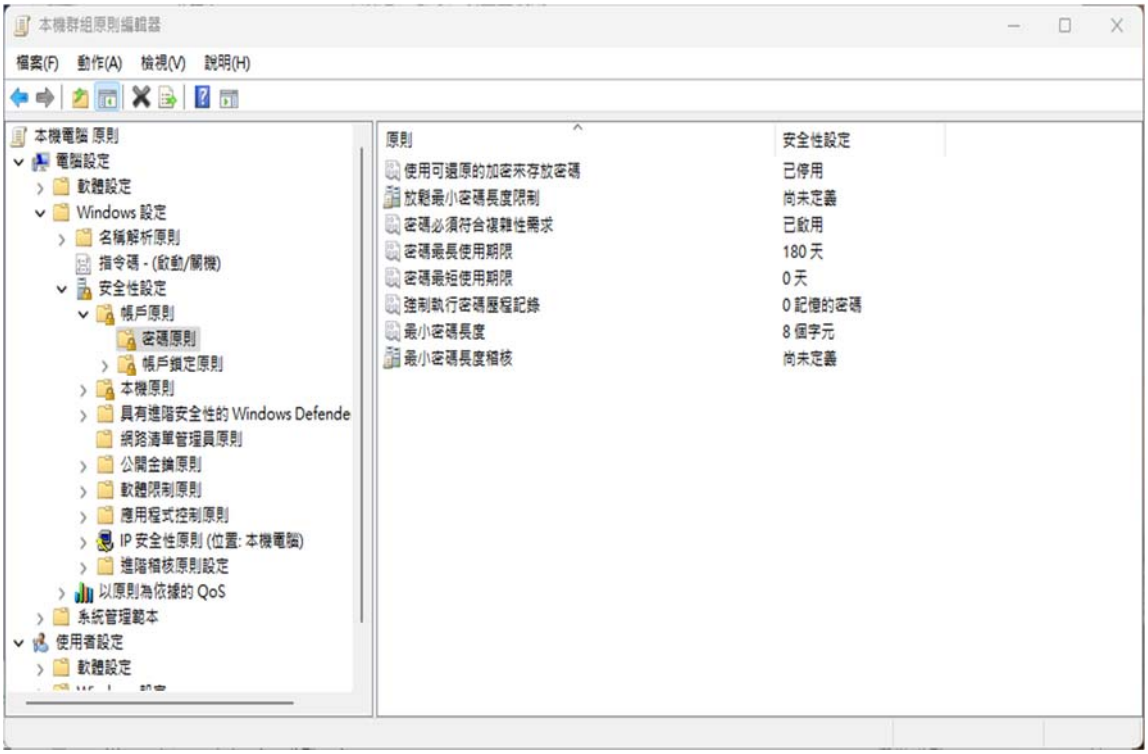
電腦設定

->Windows 設定

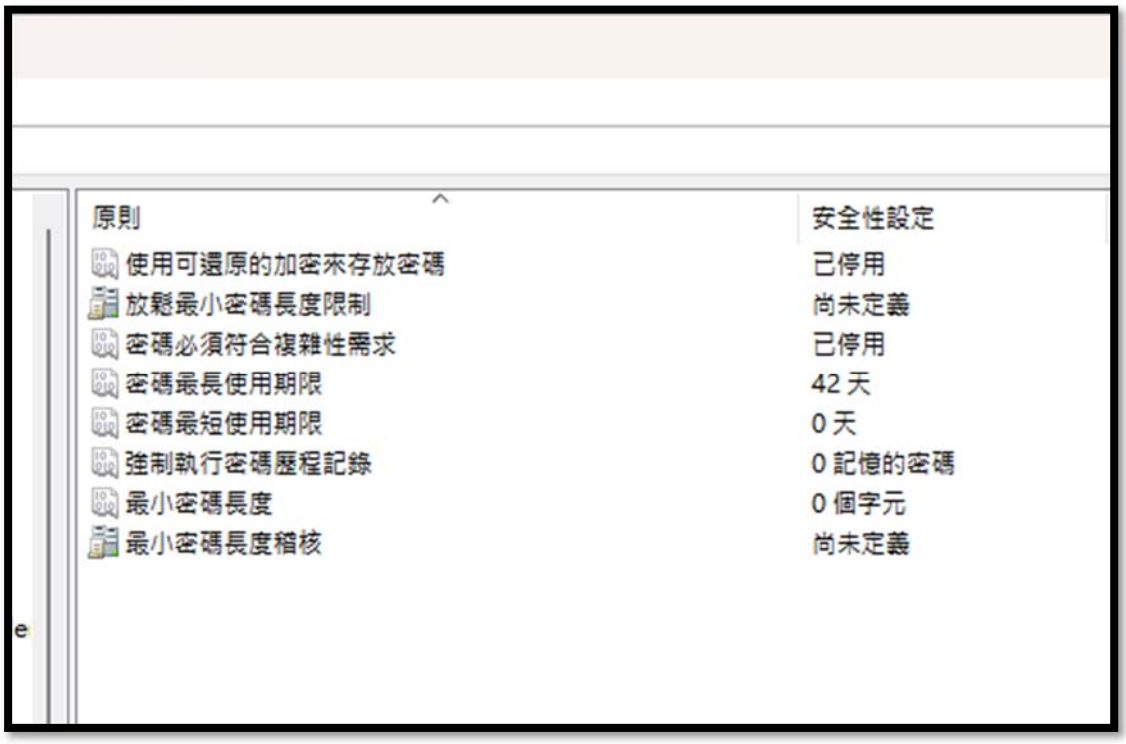
->安全性設定

->帳戶原則

->密碼原則

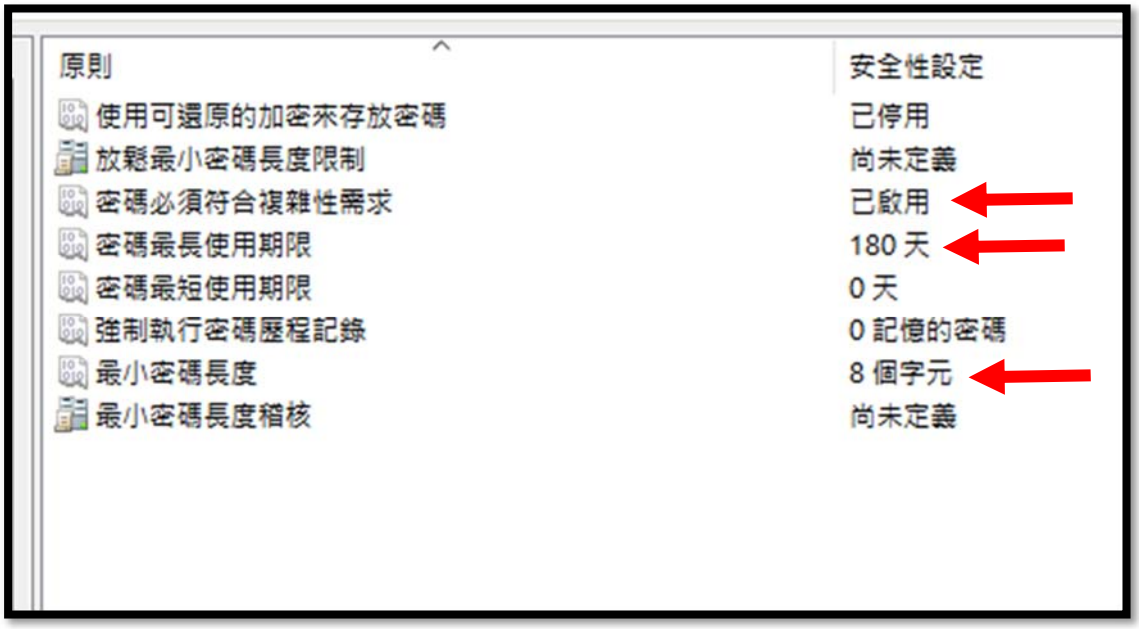


系統預設值如下



原則	安全性設定
使用可還原的加密來存放密碼	已停用
放鬆最小密碼長度限制	尚未定義
密碼必須符合複雜性需求	已停用
密碼最長使用期限	42 天
密碼最短使用期限	0 天
強制執行密碼歷程記錄	0 記憶的密碼
最小密碼長度	0 個字元
最小密碼長度稽核	尚未定義

三、修改值如下



原則	安全性設定
使用可還原的加密來存放密碼	已停用
放鬆最小密碼長度限制	尚未定義
密碼必須符合複雜性需求	已啟用
密碼最長使用期限	180 天
密碼最短使用期限	0 天
強制執行密碼歷程記錄	0 記憶的密碼
最小密碼長度	8 個字元
最小密碼長度稽核	尚未定義

四、修改項目操作及說明

項目 3. 密碼必須符合複雜性需求

這項安全性設定決定密碼是否必須符合複雜性需求。

如果啟用了此原則，則密碼必須符合下列最小需求:

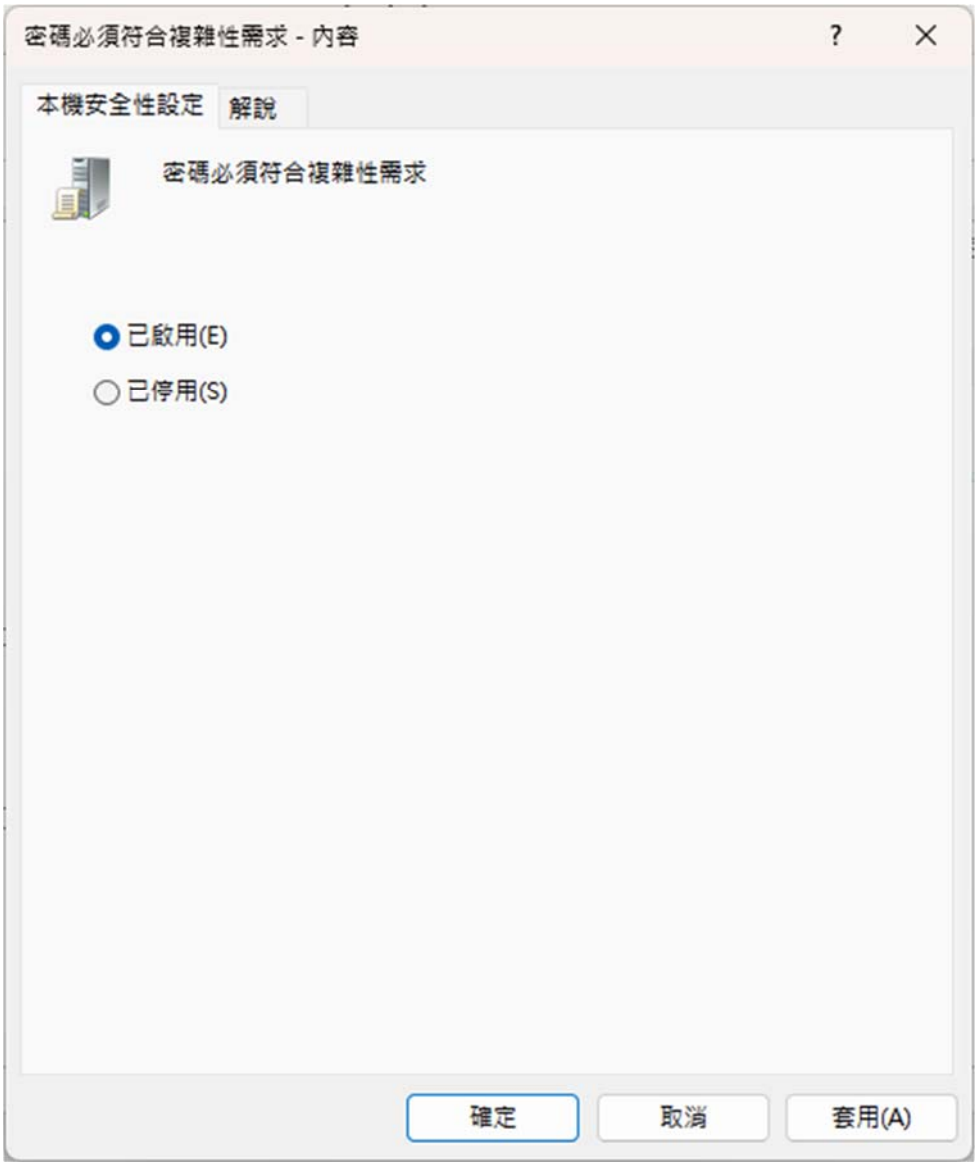
- 不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元
- 長度至少為 6 個字元
- 包含下列四種字元中的三種:
- 英文大寫字元 (A 到 Z)
- 英文小寫字元 (a 到 z)
- 10 進位數字 (0 到 9)
- 非英文字母字元 (例如: !、$、#、%)

建立或變更密碼時會強制執行複雜性需求。

預設值:

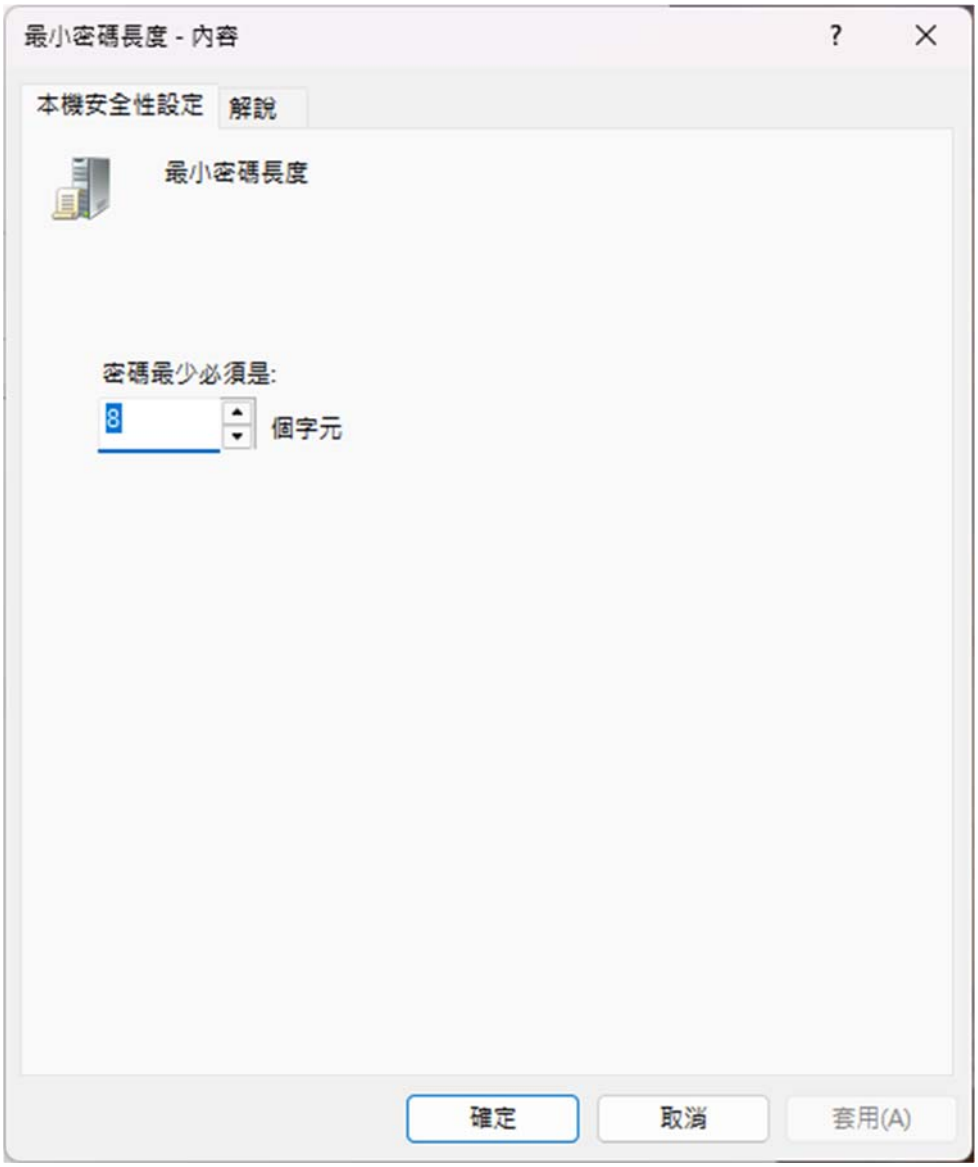
在網域控制站上為啟用。
在獨立伺服器上為停用。

注意: 根據預設，成員電腦會依循其網域控制站的設定。


密碼必須符合複雜性需求 - 內容
本機安全性設定
解說
密碼必須符合複雜性需求
已啟用(E)
已停用(S)
確定
取消
套用(A)

項目 4. 密碼最長使用期限

這項安全性設定決定系統要求使用者變更密碼之前，密碼可以使用的期限 (天數)。您可以設定密碼在 1 至 999 天之後到期; 或將天數設為 0，表示密碼永遠不會到期。如果「密碼最長使用期限」介於 1 到 999 天之間，則「密碼最短使用期限」不得超過「密碼最長使用期限」的天數。如果「密碼最長使用期限」設定為 0，則「密碼最短使用期限」可以是介於 0 到 998 天之間的任何數值。

注意: 根據您的環境而定，安全性的最佳作法是讓密碼每 30 至 90 天到期。如此一來，攻擊者破解使用者密碼及存取您的網路資源的時間便很有限。

項目 7 最小密碼長度