密碼（通行碼)設定、使用規則 ：

1. 使用者應該對持有通行碼盡保密責任

2. 通行碼設定應包含英文字及數字，長度為 8 碼（含）以上

微軟官方介紹『密碼複雜性』

https://docs.microsoft.com/zh-tw/windows/security/threat-protection/security-policy-settings/password-policy



依標題篩選
密碼原則
強制密碼歷程記錄
密碼最長使用期限
密碼最短使用期限
密碼長度下限
密碼必須符合複雜性需求
使用可還原的加密來存放密碼
帳戶鎖定原則
Kerberos 原則
稽核原則
安全性選項
進階安全性稽核原則設定
使用者權限指派
適用於企業的 Windows 安全性指導
MBSA 移除並進行替代項目
Windows 10 行動裝置版安全性指南
威脅防護的變更歷程記錄
下載 PDF

取標記的子字串。 例如，名稱 "Erin M. Hagens" 會分為三個標記： "Erin"、"M" 和 "Hagens"。 因為第二個權杖的長度只有一個字元，所以會略過。 因此，此使用者無法將密碼加上「erin」或「hagens」，以在密碼中的任何位置加入子字串。

2. 密碼包含下列其中三個類別的字元：

   - 歐洲語言的大寫字母（A 到 Z）、變音符號標記、希臘文及西瑞爾文字元（A 到 Z）
   - 歐洲語言的小寫字母（a 到 z、利 s、變音符號標記、希臘文及斯拉夫文字元）
   - 基數10位數（0到9）
   - 非數位元字元（特殊字元）：（~！ @ # $% ^& * -+ = "| \ （）{}\ [] :;" "<>,。?/）*貨幣符號（例如歐元或不列顛鎊）不會算作此原則設定的特殊字元。*
   - 歸類為字母字元但不是大寫或小寫的任何 Unicode 字元。 這包含亞洲語言的 Unicode 字元。

在變更或建立密碼時，會強制執行複雜性需求。

Windows Server 密碼複雜性需求中所包含的規則是 Passfilt 的一部分，而且無法直接修改。

啟用預設的 Passfilt 可能會針對封鎖的帳戶產生一些其他的服務台呼叫，因為使用者可能不會用來包含字母以外的字元以外的密碼。 不過，此原則設定足夠靈活，所有使用者都應該能夠透過次要學習曲線來遵守需求。

您可以在自訂 Passfilt 中包含的其他設定，就是使用非上行字元。 如果您按住 SHIFT 鍵，然後按下鍵盤 [編號] 列上的任何按鍵（從1到9和0），就可以使用列輸入字元。

可能值

- Enabled

此頁面有所助益嗎？
Yes No
本文內容
參考資料
安全性考量
相關文章

依標題篩選
密碼原則
強制密碼歷程記錄
密碼最長使用期限
密碼最短使用期限
密碼長度下限
密碼必須符合複雜性需求
使用可還原的加密來存放密碼
帳戶鎖定原則
Kerberos 原則
稽核原則
安全性選項
進階安全性稽核原則設定
使用者權限指派
適用於企業的 Windows 安全性指導
MBSA 移除並進行替代項目
Windows 10 行動裝置版安全性指南
威脅防護的變更歷程記錄
下載 PDF

可能值

- Enabled
- 已停用
- 未定義

最佳做法

> **提示**
>
> 如需最新的最佳做法，請參閱**密碼指導**方針。

將**密碼設定為必須符合複雜性需求**才能啟用。 此原則設定與 [最小密碼長度 of8] 結合，可確保單一密碼至少有218340105584896種不同的可能性。 這會使強力攻擊變得困難，但仍不可能。

使用 ALT 鍵字元組合可大大改善密碼的複雜性。 不過，如果組織中的所有使用者都符合嚴格的密碼需求，可能會導致不滿意的使用者和極為繁忙的技術支援人員。 考慮在您的組織中實現需求，在0128到0159範圍中使用 ALT 字元作為所有系統管理員密碼的一部分。 （此範圍外的 ALT 字元可以代表不會增加密碼額外複雜性的標準字母數位字元）。

只包含字母數位字元的密碼，容易受到公開使用的工具的威脅。 若要避免這種情況，密碼應該包含其他字元，並符合複雜性需求。

位置

電腦 Configuration\Windows Settings\Security Settings\Account Policies\Password 原則

此頁面有所助益嗎？
Yes No
本文內容
參考資料
安全性考量
相關文章