

Cisco WAP121和WAP321存取點上的密碼複雜性配置

目標

密碼複雜性的增加可降低安全漏洞的風險。駭客通常會在幾個小時內破解長度少於8個字元的密碼。因此，使用結合大小寫字母、數字和符號的長密碼非常重要。

本文解釋WAP121和WAP321存取點上的密碼複雜性配置。

適用裝置

- WAP121
- WAP321

軟體版本


- 1.0.3.4

密碼複雜性配置

步驟 1. 登入Web配置實用程式，選擇System Security > Password Complexity。此時將打開密碼複雜性頁：

Password Complexity

Password Complexity: ☐ Enable

Password Minimum Character Class: 

Password Different From Current: ☒ Enable


Maximum Password Length: (Range: 64 - 80, Default: 64)

Minimum Password Length: (Range: 0 - 32, Default: 8)

Password Aging Support: ☒ Enable

Password Aging Time: Days (Range: 1 - 365, Default: 180)

Password Complexity: ☒ Enable

Password Minimum Character Class: 

Password Different From Current: ☒ Enable

Maximum Password Length: (Range: 64 - 80, Default: 64)

Minimum Password Length: (Range: 0 - 32, Default: 8)

Password Aging Support: ☒ Enable

Password Aging Time: Days (Range: 1 - 365, Default: 180)

步驟 2.在「Password Complexity」欄位中選中Enable，啟用密碼複雜性。

步驟 3.從「密碼最小字元類別」下拉式清單中，選擇適當的最小字元類別數。標準鍵盤上可用的大寫字母、小寫字母、數字和特殊字元是四種可能的字元類別。

第4步：（可選）在「口令與當前口令不同」欄位中選中啟用，以要求您在當前口令過期時輸入其他口令。如果停用，您可以重新輸入您先前使用的相同密碼。

步驟 5.在「密碼長度上限」欄位中輸入密碼的最大字元數。範圍為64至80。

步驟 6.在「密碼長度下限」欄位中，輸入密碼可擁有的最少字元數。範圍為0至32。

Password Aging Support:	<input checked="" type="checkbox"/> Enable
Password Aging Time:	<input type="text" value="100"/> Days (Range: 1 - 365, Default: 180)

第7步：（可選）在Password Aging Support欄位中選中Enable，使口令在特定時間後過期。

步驟 8.如果您在上一步啟用了對密碼老化的支援，請在「密碼老化時間」欄位中輸入密碼到期的天數。範圍介於 1 至 365 天。

步驟 9.按一下Save儲存設定。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。