瞭解Cisco IOS密碼加密事實

目錄

[簡介](#)

[背景](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)
- [慣例](#)

[使用者密碼](#)

- [enable secret和enable password命令](#)
- [哪個Cisco IOS映像支援啟用金鑰？](#)
- [其他密碼](#)

[組態檔](#)

[演算法可以改變嗎？](#)

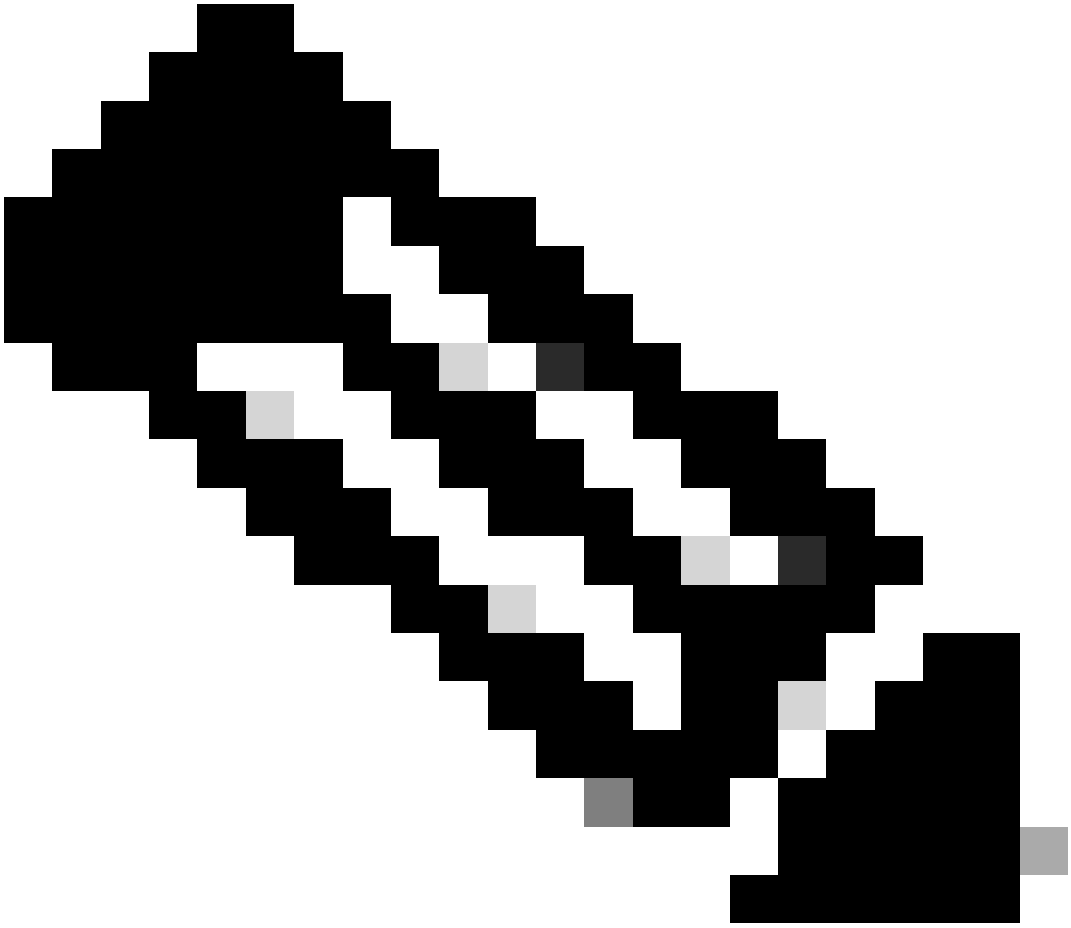
[相關資訊](#)

簡介

本檔案將說明Cisco密碼加密背後的安全模式，以及該加密的安全限制。

背景

某個思科以外的來源公佈了一項計畫，要解密思科組態檔中的使用者密碼（和其他密碼）。對於用 **enable secret** 命令設定的口令，該程式無法解密。思科使用者對該程式產生的意外擔憂，使得許多使用者懷疑思科密碼加密的安全性高於其設計目標。



注意：Cisco建議所有Cisco IOS®裝置實施身份驗證、授權和記帳(AAA)安全模型。AAA可以使用本地、RADIUS和TACACS+資料庫。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

使用者密碼

Cisco IOS配置檔案中的使用者口令和大多數其他口令(不是**enable secret**)均採用現代加密標準非常薄弱的方案加密。

雖然思科不分發解密程式，但至少有兩個不同的思科IOS密碼解密程式可供網際網路上的公眾使用；思科知道的此類程式的首次公開版本是在1995年初。我們期待任何一位業餘密碼學家都能輕而易舉地創造一個新的程式。

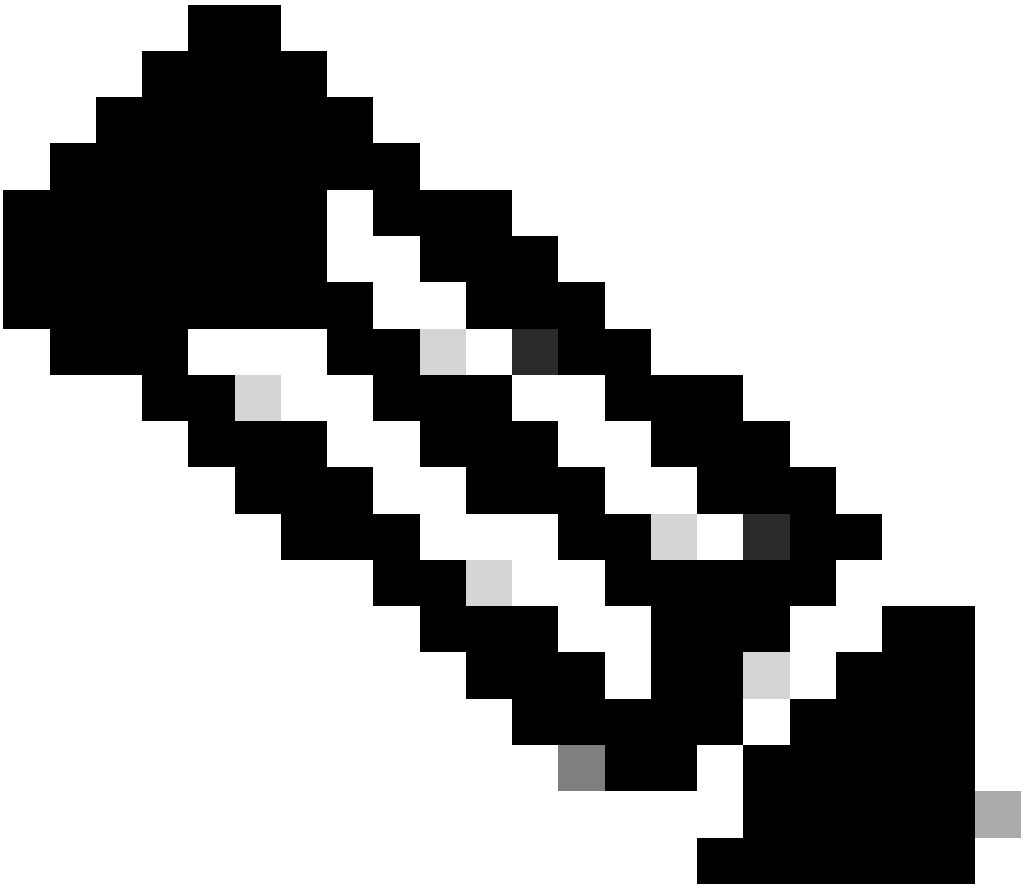
Cisco IOS用於使用者密碼的方案從來不是為了抵禦確定的智慧攻擊。加密方案旨在透過簡單的監聽或嗅探來避免密碼被盜。它從來不是為了防止有人對配置檔案執行密碼破解操作。

由於加密演算法較弱，思科始終堅持以下立場：使用者將包含口令的任何配置檔案視為敏感資訊，就像將明文口令清單視為敏感資訊一樣。

enable secret和enable password命令

不再建議使用enable password 命令。請使用enable secret命令以獲得更高的安全性。能夠測試**enable password** 命令的唯一例項是裝置處於不支援enable secret命令的引導模式時。

使用MD5演算法雜湊啟用金鑰。據思科人員所知，不可能根據配置檔案內容恢復啟用金鑰（除非明顯的詞典攻擊）。



注意：這僅適用於使用enable secret設定的口令，而不適用於使用 **enable password**設定的口令。實際上，所使用的加密強度是這兩個指令之間的唯一顯著差異。

哪個Cisco IOS映像支援啟用金鑰？

在正常操作模式下使用**show version** 命令（完整Cisco IOS映像）檢視引導映像，以確定引導映像是否支援**enable secret** 命令。如果是，請刪除 **enable password**。如果引導映像不支援 **enable secret**，請注意以下警告：

- 如果您具有物理安全性，則無需使用啟用口令，這樣任何人都無法將裝置重新載入到引導映像。

- 如果有人實際訪問裝置，他們很容易破壞裝置安全性，而無需訪問引導映像。

- 如果將**enable password** 設定為與enable secret相同，則已使enable secret與 **enable password**一樣容易遭受攻擊。

  - 如果因為引導映像不支援 **enable secret**而設定**enable password** 為其他值，則路由器管理員必須記住不常用於不支援**enable secret** 命令的ROM的新口令。使用單獨的啟用密碼時，管理員在強制執行軟體升級的停機時間時需要記住密碼，這是登入到引導模式的唯一原因。

其他密碼

Cisco IOS配置檔案中幾乎所有密碼和其他身份驗證字串都使用用於使用者密碼的弱可逆方案加密。

要確定已使用哪種方案來加密特定口令，請在配置檔案中檢查加密字串之前的位數。如果該數字為7，則口令已使用弱演算法加密。如果數字是5，則密碼已使用更強大的MD5演算法進行了雜湊處理。

例如，在配置命令中：

```
<#root>
```

enable secret 5 1iUjJ$cDZ03KKGh7mHfX2RSbDqP.

Enable secret已使用MD5進行雜湊處理，但在命令中：

<#root>

username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D

密碼已使用弱可逆演演算法加密。

組態檔

當您以電子郵件傳送組態資訊時，請使用型別7密碼來清除組態。預設情況下，您可以使用show tech-support命令對資訊進行清除。**show tech-support** 命令輸出的示例如下所示：

<#root>

```
...
 hostname routerA
 !
 aaa new-model
 aaa authentication login default local
 aaa authentication ppp default if-needed local
```

enable secret 5 <removed>

```
 !
```

```
username jdoe password 7 <removed>
username headquarters password 7 <removed>
username hacker password 7 <removed>



...
```

將組態檔儲存在簡單式檔案傳輸通訊協定(TFTP)伺服器上時，請變更該檔案未使用時的許可權，或將其放在防火牆之後。

演算法可以改變嗎？

思科目前沒有計畫支援對Cisco IOS使用者密碼使用更強大的加密演算法。如果思科確實決定將來引入此類功能，則該功能無疑會給選擇使用該功能的使用者帶來額外的管理負擔。

在一般情況下，不可能將使用者密碼切換到用於使能加密的基於MD5的演算法，因為MD5是單向雜湊，並且密碼根本無法從加密資料恢復。為了支援某些身份驗證協定（特別是CHAP），系統需要訪問使用者密碼的明文，因此必須使用可逆演算法儲存這些密碼。

金鑰管理問題會使切換到更強的可逆演算法(如資料加密標準(DES))成為一項不繁瑣的任務。雖然使用DES加密口令很容易修改Cisco IOS，但是如果所有Cisco IOS系統都使用相同的DES金鑰，這種方法就不會有安全性優勢。如果不同系統使用不同的金鑰，將會給所有Cisco IOS網路管理員帶來管理負擔，並且會破壞系統之間配置檔案的便攜性。使用者對更強的可反轉密碼加密的需求一直很小。

相關資訊

- **密碼復原程序**
- **用來強化 Cisco IOS 裝置的思科指南**
- **技術支援 - Cisco Systems**

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）。