了解Cisco IOS密码加密相关信息

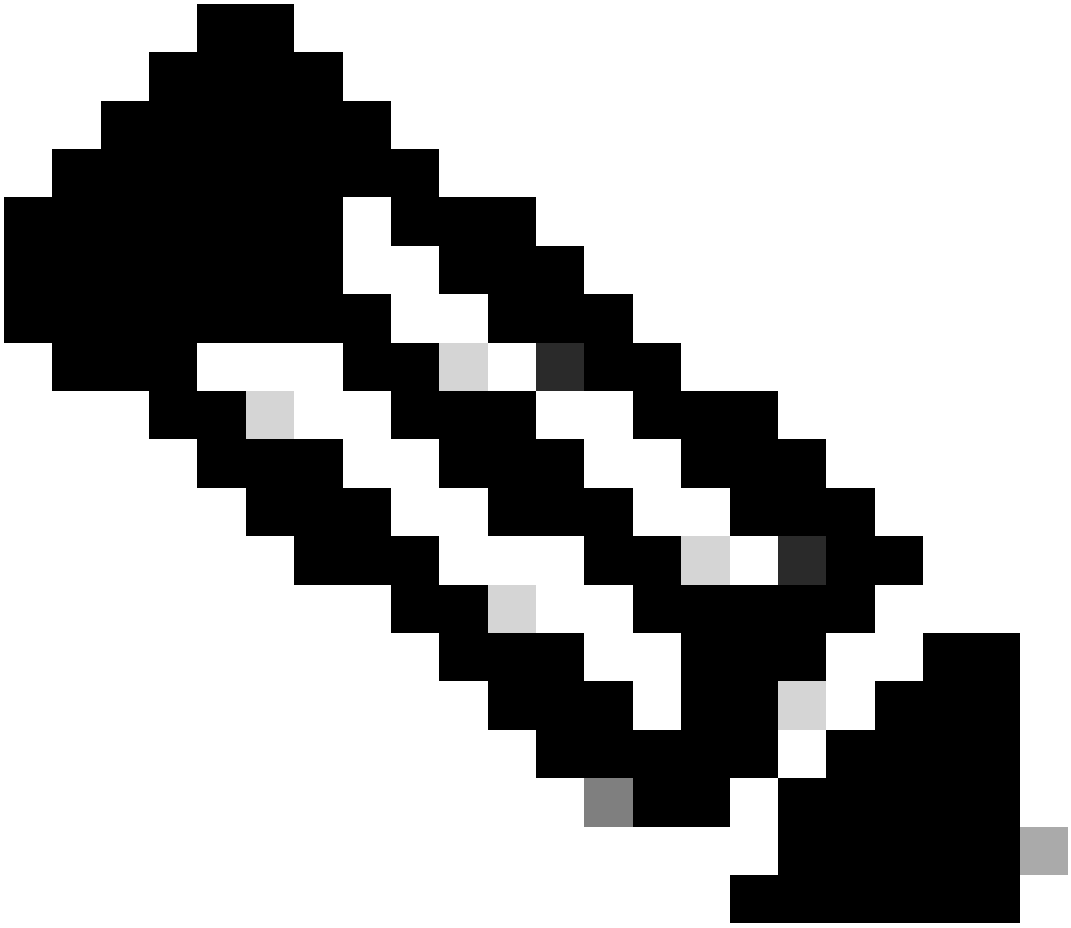
目录

简介

本文档介绍Cisco密码加密背后的安全模型，以及该加密的安全限制。

背景

某非 Cisco 来源发布了对 Cisco 配置文件中的用户口令（及其他口令）进行解密的程序。对于用 **enable secret** 命令设置的口令，该程序无法解密。思科用户对该程序产生的意外顾虑，已导致许多用户怀疑思科密码加密所提供的安全性高于其设计初衷。



注意：思科建议所有Cisco IOS®设备实施身份验证、授权和记帐(AAA)安全模型。AAA 可以使用本地、RADIUS 和 TACACS+ 数据库。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

用户密码

Cisco IOS配置文件中的用户口令和大多数其他口令(不是**enable secret**)都采用现代加密标准中非常薄弱的方案进行加密。

虽然思科不分发解密程序，但至少有两个不同的思科IOS密码解密程序可供互联网上的公众使用；思科知道的此类程序的第一个公开版本是在1995年初。我们希望所有业余密码学家都能轻而易举地创造出一个新的程序。

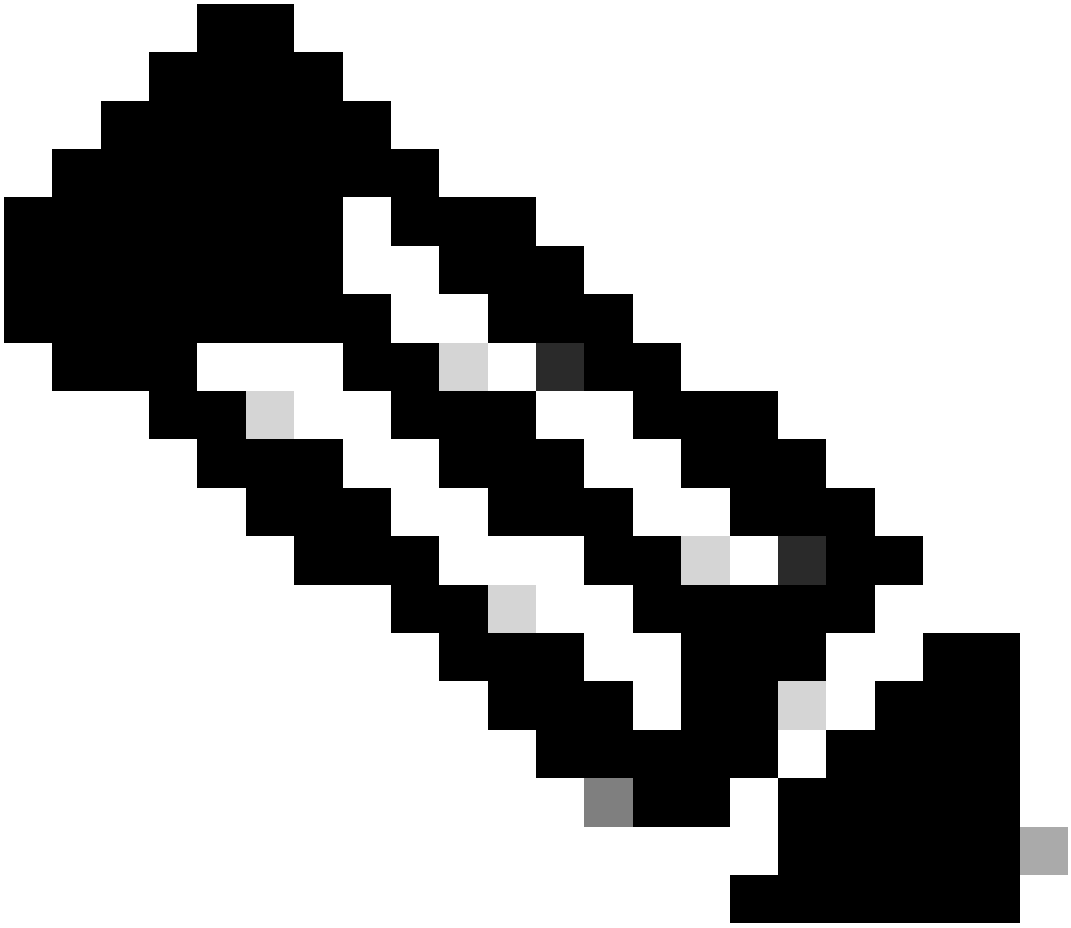
Cisco IOS用于用户密码的方案绝不是为了抵御坚决的智能攻击。加密方案旨在通过简单的监听或嗅探来避免密码失窃。它绝不是为了防止有人对配置文件执行密码破解操作。

由于加密算法较弱，思科一直主张用户将包含密码的任何配置文件视为敏感信息，就像处理密码的明文列表一样。

enable secret和enable password

不建议再使用enable password 命令。请使用enable secret命令以获得更高的安全性。唯一可以测试**enable password** 命令的实例是设备处于不支持enable secret命令的引导模式时。

使用MD5算法散列启用密钥。据Cisco的任何人员所知，不可能根据配置文件的内容恢复使能加密口令（除非明显的字典攻击）。



注意：这仅适用于使用enable secret设置的口令，而不适用于使用 **enable password**设置的口令。实际上，所用加密的强度是这两个命令之间的唯一显著差异。

哪个Cisco IOS映像支持enable secret？

在正常操作模式下使用**show version** 命令（完全Cisco IOS映像）查看您的引导映像，以查看引导映像是否支持**enable secret** 命令。如果是，请删除 **enable password**。如果引导映像不支持 **enable secret**，请注意以下警告：

- 如果您具有物理安全性，则无需使用启用密码，这样便没有人可以将设备重新加载到引导映像。

- 如果有人对设备有物理访问，则无需访问引导映像，即可轻松破坏设备安全性。

- 如果将**enable password** 设置为与enable secret相同，则已使enable secret与 **enable password**一样容易遭受攻击。

  - 如果因为引导映像不支持 **enable secret**而将**enable password** 设置为不同的值，则路由器管理员必须记住新口令，该口令会在不支持**enable secret** 命令的ROM上被频繁使用。使用单独的启用密码时，管理员在强制软件升级中断时需要记住该密码，这是登录到引导模式的唯一原因。

其他密码

Cisco IOS配置文件中的几乎所有密码和其他身份验证字符串都使用用于用户密码的弱可逆方案加密。

要确定已使用哪种方案加密特定密码，请在配置文件中检查加密字符串之前的数字。如果该数字是7，则密码已使用弱算法加密。如果数字是5，则密码已使用更强大的MD5算法进行了哈希处理。

例如，在配置命令中：

```
<#root>
```

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
```

enable secret has been hashed with MD5，而在该命令中：

<#root>

username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D

密码已使用弱可逆算法加密。

配置文件

当您通过电子邮件发送配置信息时，请清除第7类密码中的配置。您可以使用show tech-support命令，该命令在默认情况下对信息进行清理。**show tech-support** 命令输出的示例如下所示：

<#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>
```

```
...
```

在简单文件传输协议(TFTP)服务器上保存配置文件时，请更改该文件在不使用时的权限或将其置于防火墙之后。

算法可以改变吗？

Cisco目前没有计划支持更强的Cisco IOS用户密码加密算法。如果思科决定将来引入此类功能，则该功能无疑会为选择使用该功能的用户带来额外的管理负担。

在一般情况下，不可能将用户密码切换到用于使能加密的基于MD5的算法，因为MD5是单向散列，并且无法从加密数据中恢复密码。为了支持某些身份验证协议（特别是CHAP），系统需要访问用户密码的明文，因此必须使用可逆算法存储这些密码。

密钥管理问题意味着切换到更强的可逆算法（如数据加密标准[DES]）是一项非常艰巨的任务。虽然修改Cisco IOS以使用DES加密口令比较容易，但如果所有Cisco IOS系统都使用相同的DES密钥，则此方法不会具有安全优势。如果不同的系统使用不同的密钥，将会给所有Cisco IOS网络管理员带来管理负担，并且会破坏系统之间的配置文件可移植性。用户对于更强的可逆密码加密的需求一直很小。

相关信息

- 密码恢复规程
- **硬化Cisco IOS设备的Cisco指南**
- **技术支持 - Cisco Systems**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。