



方位配置文件加密介绍

版本：〈1.1〉

发布日期：〈2018-5-11〉



目录

1	修订历史.....	2
2	介绍.....	3
2.1	概述.....	3
2.2	适用型号.....	3
2.3	目标受众.....	3
3	如何对配置文件进行加密.....	4
4	如何在批量部署中使用加密的配置文件.....	7

1 修订历史

修订历史:

版本	作者	发布时间	说明
1.1	岳洋	2018.5.11	初始版本

2 介绍

2.1 概述

由于批量部署的便捷性，越来越多的客户使用这一种方式来部署话机。但是，在批量部署的过程中，配置文件不可避免的会在网络中进行传输。配置文件中有很多的敏感信息，例如：SIP 帐号和密码，话机的密码，网络电话本的帐号信息等。

为了避免信息外泄，我们可以使用加密工具来对配置文件进行加密。这个文档主要介绍如下两部分：

- A、 如何对配置文件进行加密
- B、 如何在批量部署中使用加密的配置文件

2.2 适用型号

本档适用于 Fanvil 全系列话机。

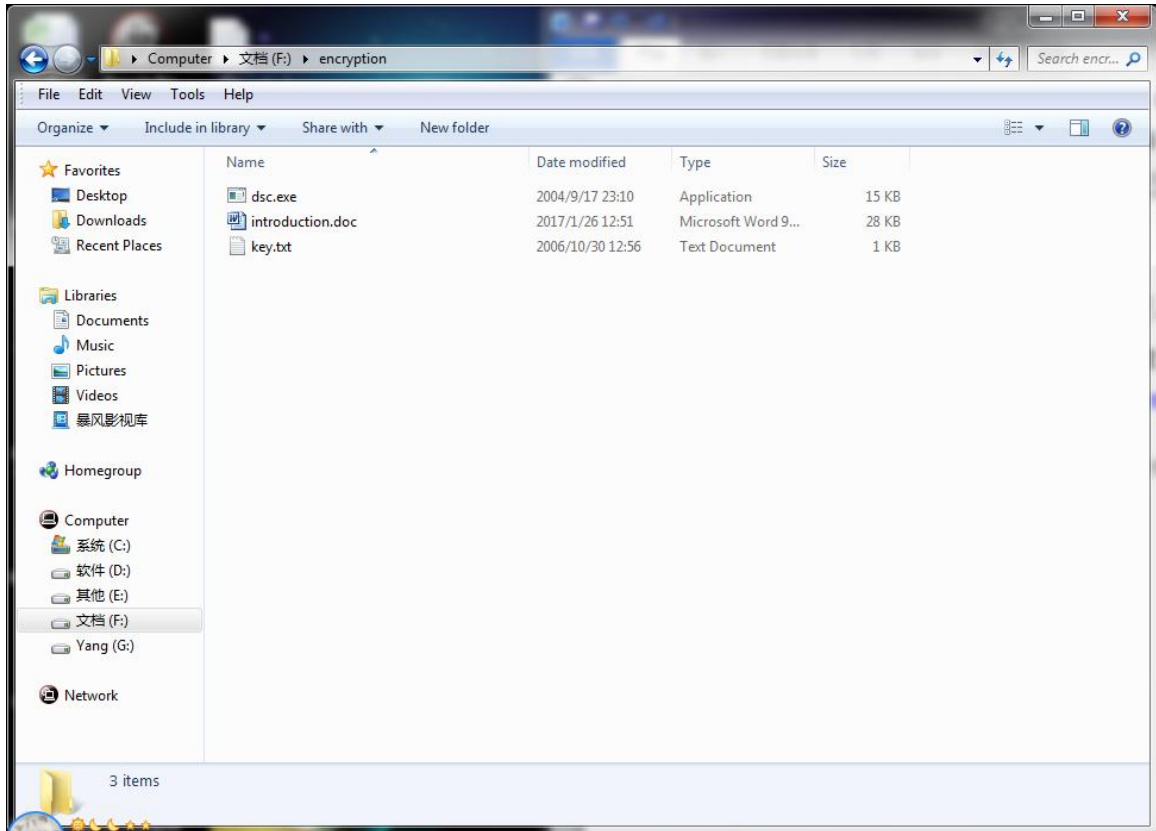
2.3 目标受众

此文档是针对那些想了解配置文件加密功能的公司内部研发或者测试人员。

3 如何对配置文件进行加密

我们可以使用 DSC 工具来对配置文件进行 AES256 的加密。该工具可以从 <http://download.fanvil.com/tool/AES%20tool/encryption.7z> 中进行下载。下面通过一个例子来讲述如何进行配置文件加密。

1) DSC 工具下载完成后解压，并将文件夹放在 F 盘下，

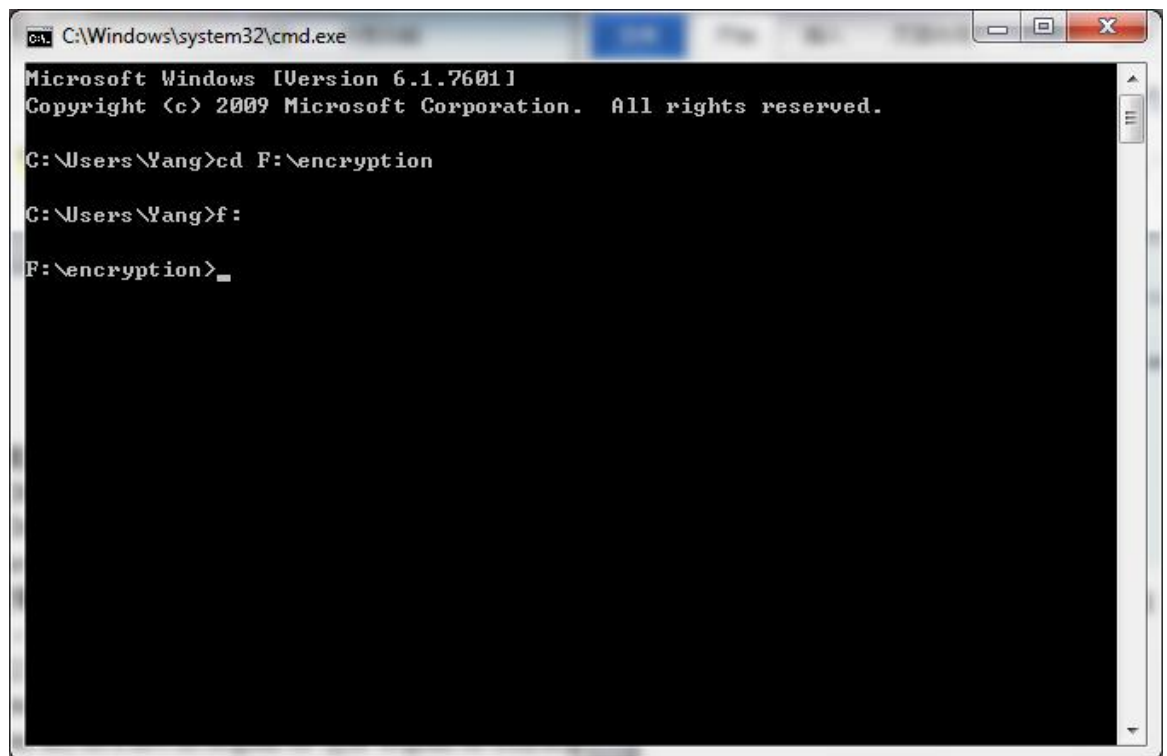


2) 然后打开 key.txt，使用默认的或者自己重新输入随机的 64 位密钥，都可以。然后保存。

3) 从话机的网页中下载配置文件，并且将相关的信息修改完成。文件名字为 config.txt. 将其放在 F 盘，encryption 目录下。



4)在运行中输入 cmd 进入 Dos 命令行。然后通过下图中的命令进入 encryption 目录



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Yang>cd F:\encryption

C:\Users\Yang>f :

F:\encryption>_
```

5) 使用如下命令对文件进行加密或者解密

加密: dsc.exe key.txt e config.txt encrypted.txt

dsc.exe : 工具名

key.txt : 密钥文件

“e” : 表示加密,

config.txt : 配置文件名字

encrypted.txt : 加密之后生成的文件, 名字可以自定义。

解密: dsc.exe key.txt d encrypted.txt original.txt

dsc.exe : 工具名

key.txt : 密钥文件

“d” : 表示解密,

encrypted.txt : 加密文件的名字

original.txt : 解密之后生成的文件, 名字可以自定义。

```
ca. C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Yang>cd F:\encryption
C:\Users\Yang>f:
F:\encryption>dsc.exe key.txt e config.txt encrypted.txt
DONE 0MB
F:\encryption>dsc key.txt d encrypted.txt original.txt
DONE 0MB
F:\encryption>
```

加密的文件

解密之后的文件

4 如何在批量部署中使用加密的配置文件

如果希望使用加密的配置文件对话机进行升级，需要在话机的网页中添加密钥。如下图所示：



最后将 2 中生成的加密配置文件放入文档服务器，在话机上设置好文档服务器的相关信息即可。具体信息参考《[Auto Provision 的机制、环境搭建、配置文件说明](#)》。