Fanvil configuration file encryption introduction

Version: <1.1>
Release date: <2018-5-11>

Contents

1 Introduction

1.1 Summary

As the convenience of auto provision way, there are more and more customers use it to deploy the IP phones. However, during the procedure of autoprovision, the configuration file must be sent via the LAN or WAN. It contains various sensitive private information, such as SIP account, password, phone administrator password, and so on.

In order to avoid information leakage, we could use a software named dsc.exe to encrypt the configuration file with AES256. It could be downloaded from http://download.fanvil.com/tool/AES%20tool/dsc.exe.

This document is used to introduce the following two usages.

A. How to encrypt the configuration file of Fanvil products

B. How to use the encrypted configuration file in the autoprovision procedure

1.2 Model

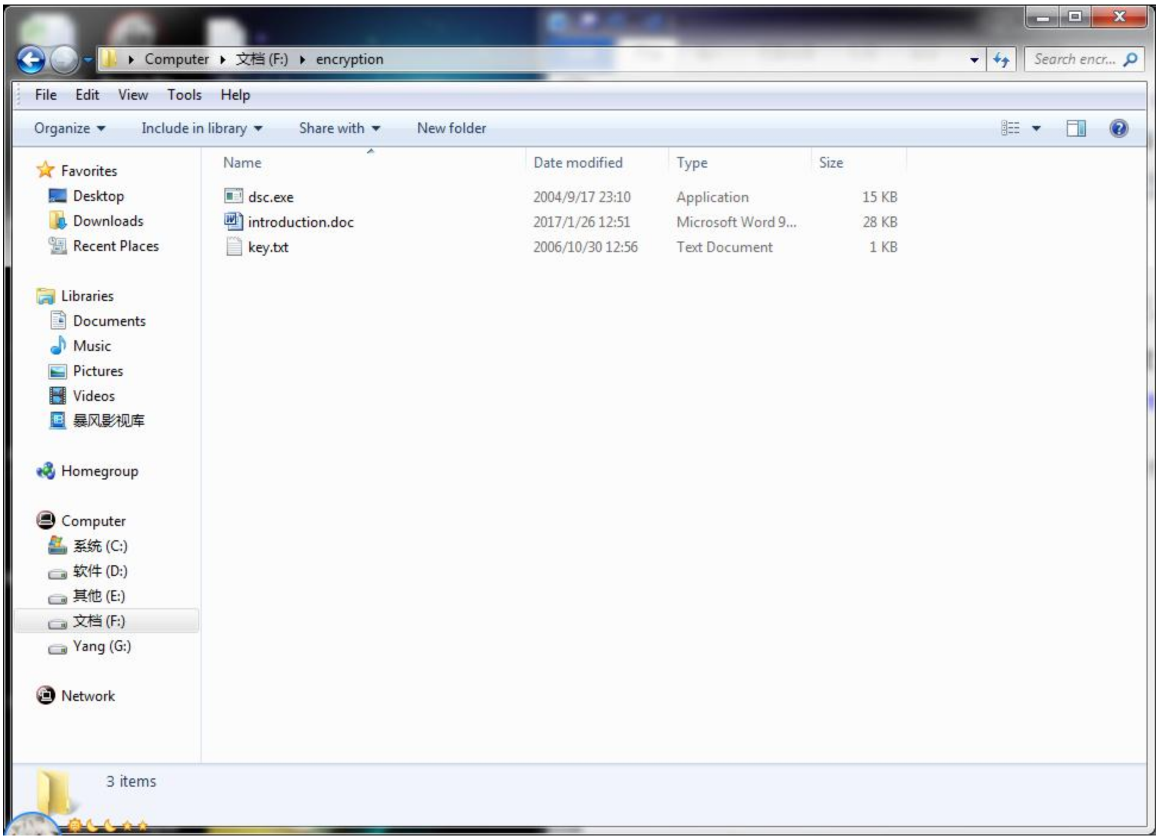
This instruction is available for all the Fanvil IP phones.

2 How to encrypt the configuration file of Fanvil products

2.1 How to configure encrypted files under Windows

We could use DSC to encrypt the configuration files with AES 256. It could be got fromhttp://download.fanvil.com/tool/AES%20tool/encryption.7z. Now, there is an example to display how to do the encryption operation.

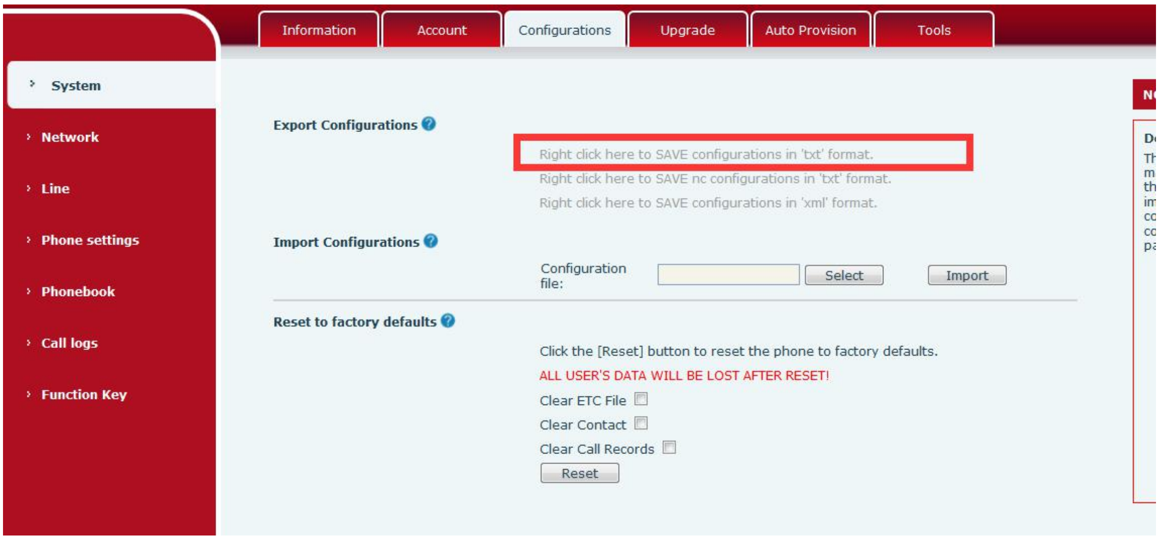
1) After unzipping the encryption.7z file, please put in into F disk root path.



Name	Date modified	Type	Size
dsc.exe	2004/9/17 23:10	Application	15 KB
introduction.doc	2017/1/26 12:51	Microsoft Word 9...	28 KB
key.txt	2006/10/30 12:56	Text Document	1 KB

2) Open key.txt, and the encryption key is in it. Customers could use the default value or type a new one. Note that the key must be 64 characters.

3) Download the configuration file on phone webpage, and modify it with the necessary information. As default, the name is config.txt. Put it into F:\encryption\



Export Configurations

Right click here to SAVE configurations in 'txt' format.

Right click here to SAVE nc configurations in 'txt' format.

Right click here to SAVE configurations in 'xml' format.

Import Configurations

Configuration file:

Reset to factory defaults

Click the [Reset] button to reset the phone to factory defaults.

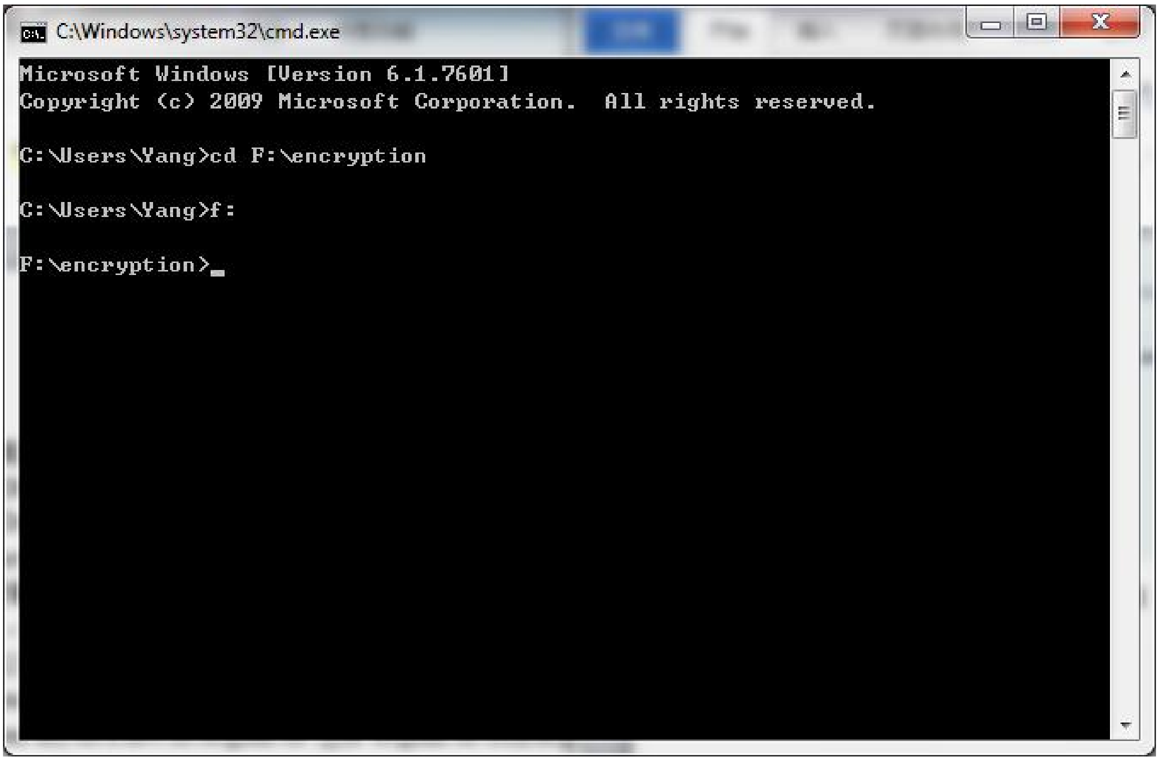
ALL USER'S DATA WILL BE LOST AFTER RESET!

Clear ETC File □

Clear Contact □

Clear Call Records □

4) Search cmd in Windows system and go to the Dos command window. Type the command in following picture to enter encryption path.



```
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) Use the follow command to encrypt or decrypt the file.

Encrypt command: dsc.exe key.txt e config.txt encrypted.txt

dsc.exe: tool name

key.txt: encryption key file

"e": means encrypt

config.txt: configuration file name

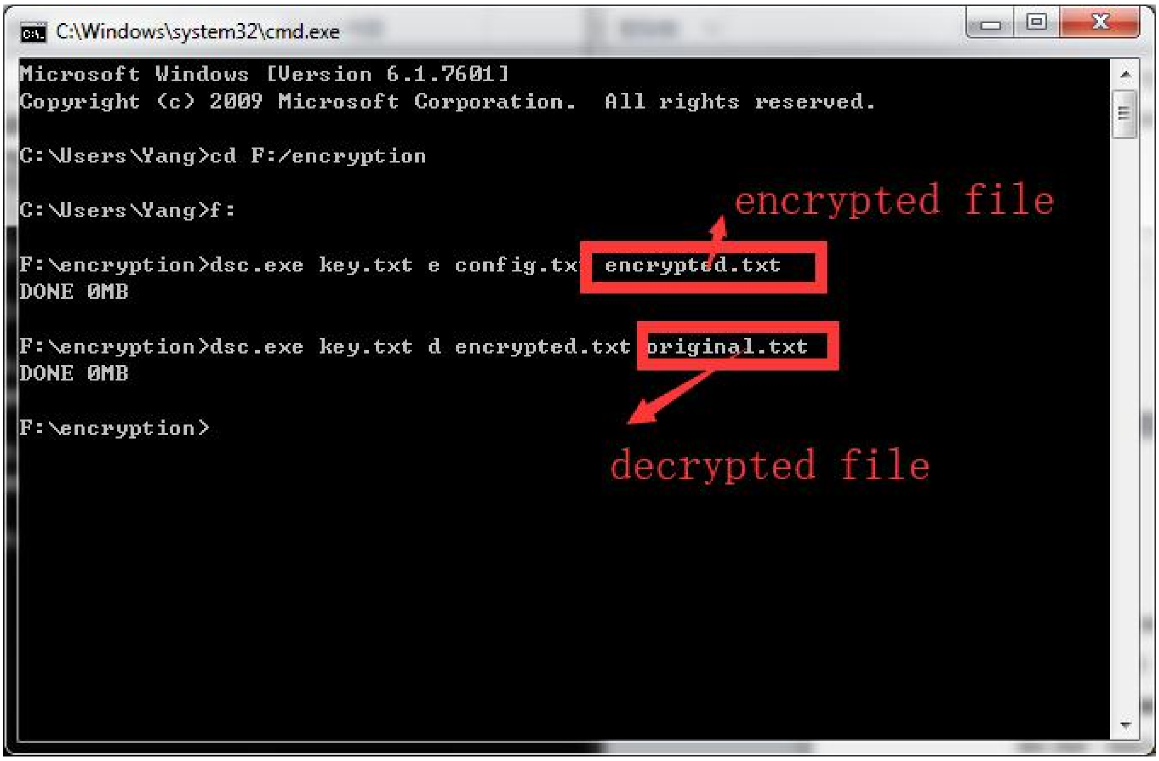
encrypted.txt: the made file by the tool. It is the encrypted file.

Decrypt command: dsc.exe key.txt d encrypted.txt original.txt

dsc.exe: tool name

key.txt: decryption key file

"d": means decryption
encrypted.txt: the encrypted file name
original.txt: the made file by the tool. It is the decrypted file.

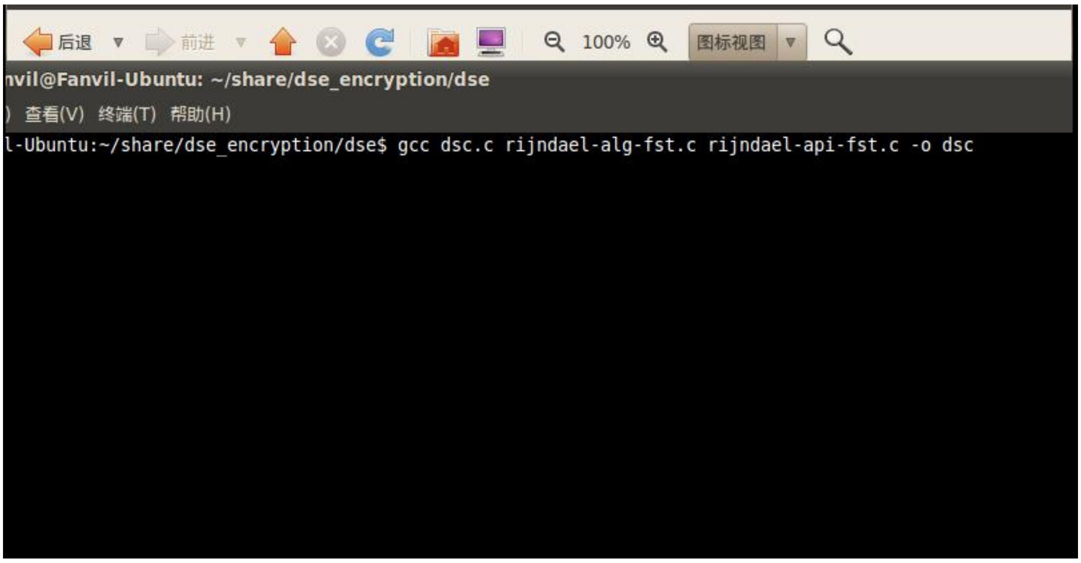


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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.exe key.txt d encrypted.txt original.txt
DONE 0MB

F:\encryption>
```

2.2 How to configure encrypted files under Linux

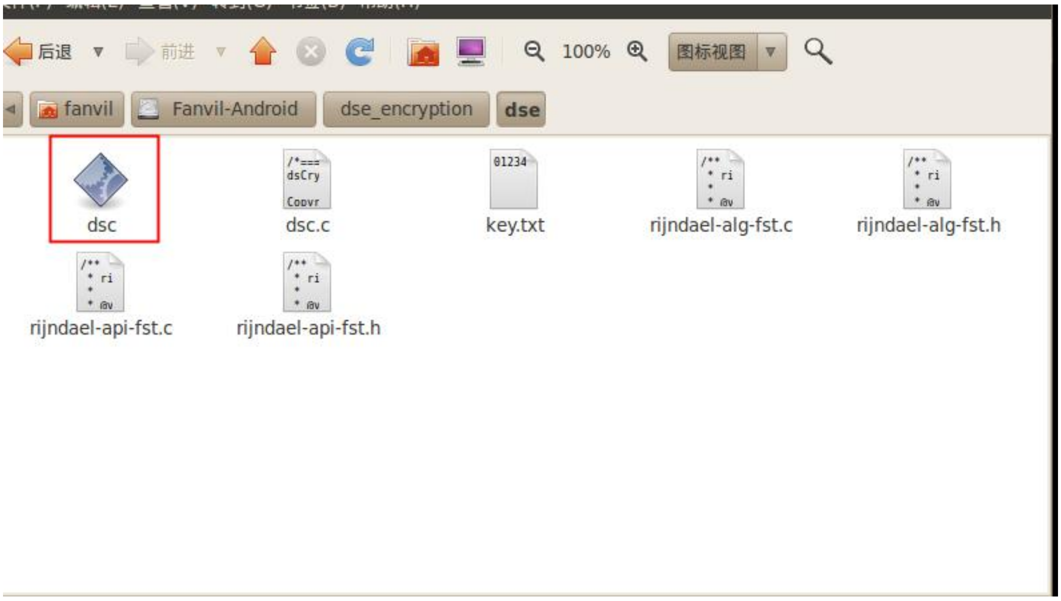
1) Download the below link
https://1drv.ms/u/s!AhLXW_VNOC9LgR6TiW5931ydvEP5

2) After downloading, unzip it into Linux, and then go to the relevant path to execute the compile command to obtain DSC tools.
gcc dsc.c rijndael-alg-fst.c rijndael-api-fst.c -o dsc

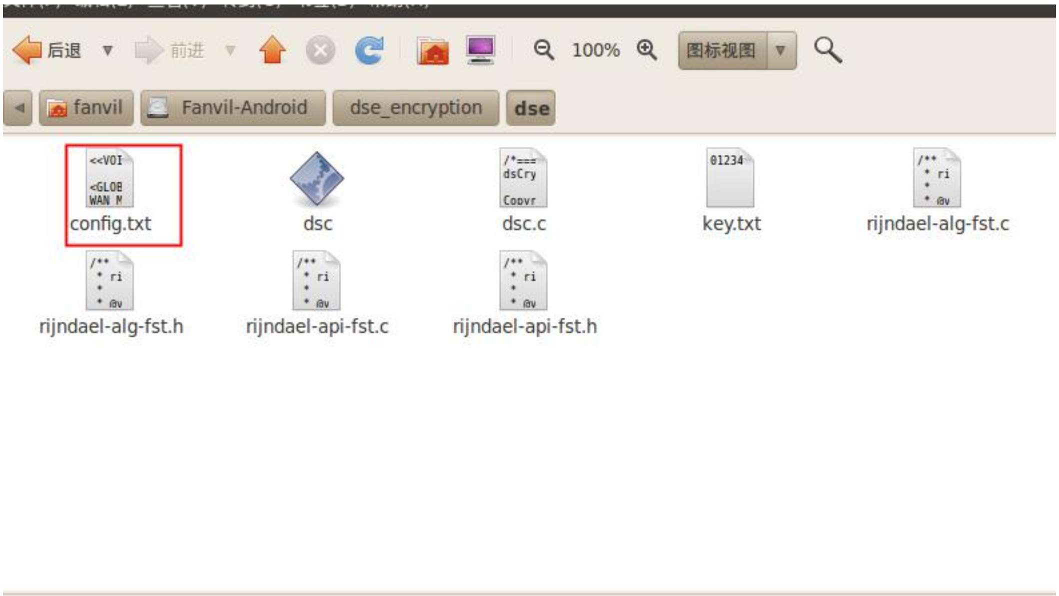


```
nvil@Fanvil-Ubuntu: ~/share/dse_encryption/dse
) 查看(V) 终端(T) 帮助(H)
l-Ubuntu:~/share/dse_encryption/dse$ gcc dsc.c rijndael-alg-fst.c rijndael-api-fst.c -o dsc
```

3) After excution,will generates DSC tools(refer t the below picture)



4) Then put the encrypted file or decryped file in the path of dse.



5）Encryption command：

dsc a:\my.key e d:\x\data.zip data.enc（for example：dsc key.txt e config.txt encryption.enc）

dsc:tools

key.txt：key

e：encryption

Config.txt:Files that need to be encrypted

encryption.enc:Encrypted file

6）Decryption command：

dsc my.key d data.enc c:\tmp\data.zip（for example：dsc key.txt d encryed.txt config_after.txt）

dsc:tools

key.txt：key

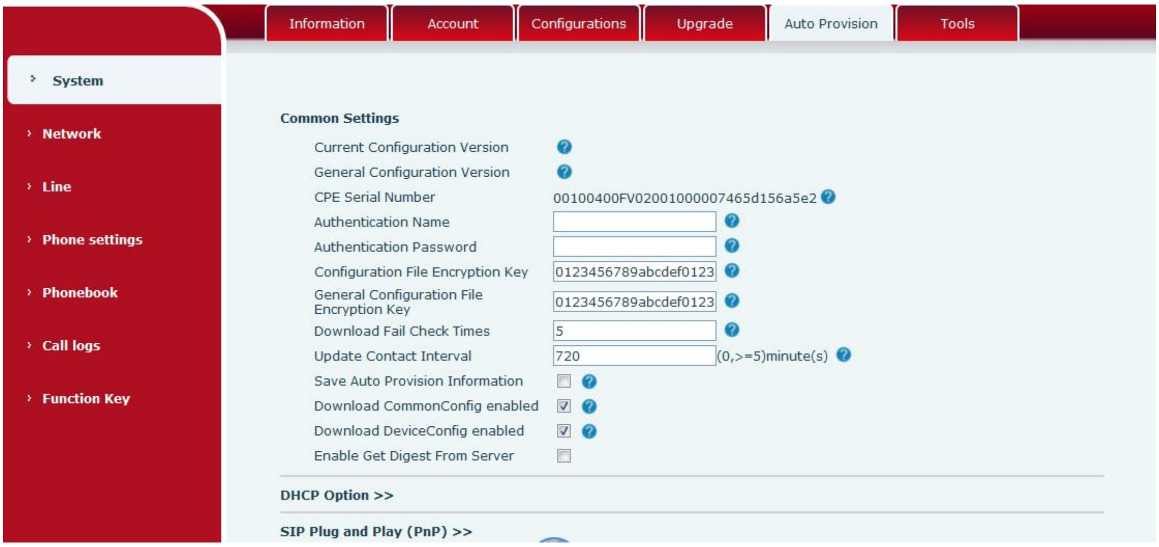
d：decryption

encryed.txt:Files to be decrypted

Config_after.txt:Decrypt the file

3 How to use the encrypted configuration file in the auto-provision procedure

If customers want to use encrypted configuration file to configure the IP phone, adding the key is necessary operation. Customers could add it on the following page.



Common Settings

Current Configuration Version	
General Configuration Version	
CPE Serial Number	00100400FV02001000007465d156a5e2
Authentication Name	
Authentication Password	
Configuration File Encryption Key	0123456789abcdef0123
General Configuration File Encryption Key	0123456789abcdef0123
Download Fail Check Times	5
Update Contact Interval	720 (0,>=5)minute(s)
Save Auto Provision Information	□
Download CommonConfig enabled	☑
Download DeviceConfig enabled	☑
Enable Get Digest From Server	□

DHCP Option >>

SIP Plug and Play (PnP) >>

Finally, put the file made in 2 into configuration file server and type the server information on phone webpage. For details, refer to Autoprovision introduction.