

Cleo[®] Host Loginid Import Utility
and
Cleo[®] Host Password Encryption Utility
User Guide

INTRODUCTION	3
Overview	3
Intended Audience	3
LOGIN ID IMPORT UTILITY	4
HOST ENCRYPTED PASSWORD UTILITY	5
INSTALLATION.....	7
Avaya IR R1.1/R1.2/R1.3	7
Installation from CPIO Image.....	8
Installation from CD	10
GETTING STARTED	12
Obtain & Register A License Key	12
Instructions for Installing the License	12
Instructions for Enabling the Encrypted Password Feature	14
Instructions for Using the Encrypted Password Feature.....	15
USING THE CLEO HOST LOGIN ID IMPORT UTILITY	17
UNDERSTANDING THE AVAYA MASTER LOG MESSAGES REPORT FOR THE CLEO HOST LOGINID IMPORT AND THE CLEO HOST PASSWORD ENCRYPTION UTILITIES	22
MESSAGES.....	22
EXAMPLE of AVAYA MASTER LOG MESSAGES	24
TROUBLE SHOOTING	25
APPENDIX A.....	27

Introduction

Overview

On the Avaya IVR systems which require host access there are host maintenance scripts that perform the necessary host login functions for each session as part of the process of parking each session at the appropriate screen for handling host transactions required for incoming calls. The login ID and password combinations are stored on the Avaya IVR systems in clear text files. Many institutions who manage sensitive information and who also guarantee the security of this information to their respective clients do not consider this scenario to meet their requirements.

In response to their concerns Cleo has developed the password encryption feature that is an add-on feature to the Cleo Host Interface products. This feature allows IVR system administrators to establish passwords and have them stored in an encrypted file. This feature goes a step further and also stores the Logon IDs in an encrypted file as well. The encryption used is RC4 128 bit key encryption algorithm.

NOTE: Due to United States Export Laws, the encryption used may be RC4 56 bit key encryption algorithm, based on the Country the Cleo Host Interface product is used in.

Two utilities are provided to support password encryption on the Avaya IVR platform.

hlogidimport	create initial encrypted password file for an application.
hpwencrypt	create/modify login ids and/or passwords in an application's encrypted password file

It is important to note that these utilities do not affect logon ids and passwords values stored on the mainframe. Any changes made to logon ids and passwords on the Avaya IVR system using these utilities must be coordinated with the respective changes on the mainframe or midrange system.

Intended Audience

The intended audience of this document is presumed to be familiar with the features and operation of the Avaya IR system and the Cleo Host Interface software on the Avaya VR system.

This utility is targeted for use by IVR application developers and system administrators that need access to mainframe 3270 host applications and require a higher level of security than what is provided by storing login ids and passwords in clear text files.

Login ID Import Utility

The Cleo Host Login ID Import Utility is a command line application that will create an initial encrypted loginid, NULL password file. Typically, the Host Loginid Import Utility is used before using a Cleo custom Host Password Update Utility or the Cleo Host Password Encryption Utility, to create an encrypted password file that can be used by the Cleo Host DIP.

Using the Host Loginid Import Utility saves the user the time and effort of inputting a Loginid for each Avaya IR Session, when creating an encrypted loginid, password file.

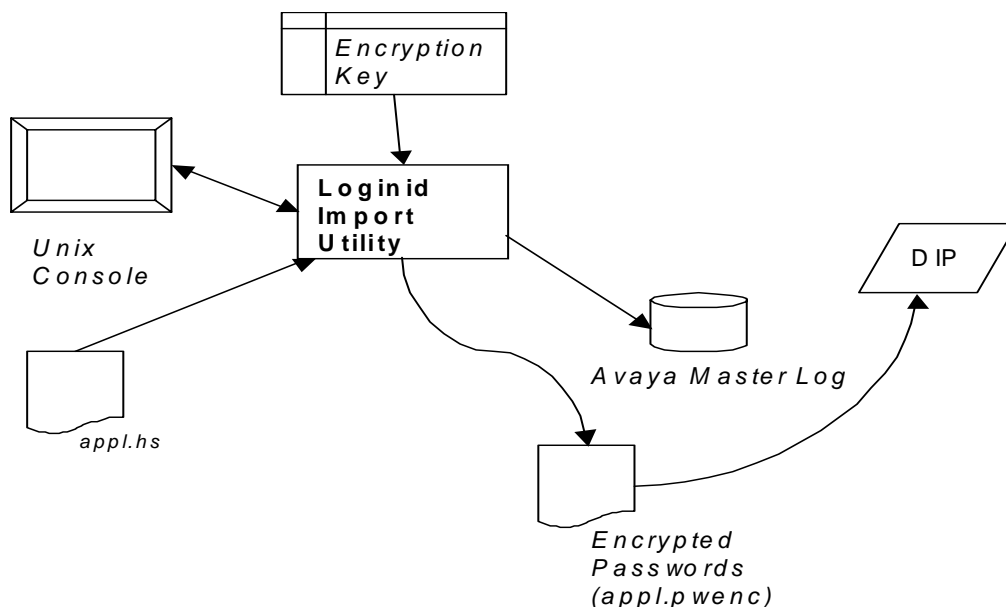


Figure 1 - Login ID Import Utility functional components

Host Login ID Import Utility functions:

1. Import all of the login ID's from a specified IVR Designer, Voice@Work, or Script Builder application's Host Maintenance Script file(<application name>.hs).
2. Use the number of login ID's defined in the Application's Host Maintenance Script (<application name>.hs) file to determine the number of Host Sessions for which to define a login id, password pair.
3. Create an encrypted file comprised of each login id, password pair.
4. Report the number of login ids that were imported.
5. Log error messages to the Avaya Master LOG, so that the Avaya "display messages" command can be used by the System Administrator to report any Host Loginid Import Utility errors.

Host Encrypted Password Utility

The Cleo Host Password Encryption Utility is a command line application that will create or modify an encrypted password file that can be used by the Cleo Host DIP.

The Host Password Encryption Utility allows a user to define 1 password, or individual passwords for a range of Avaya IR Host Sessions. The Loginid associated with each Host Session can be optionally input by the user, or read from the existing encrypted password file.

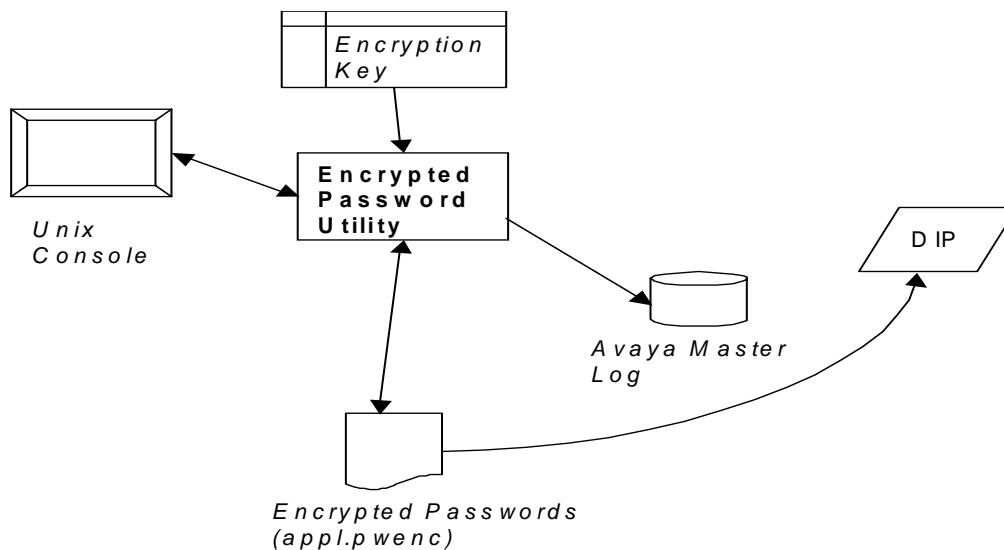


Figure 2 - Host Password Encryption Utility Functional Components

Host Password Encryption Utility functions:

1. Allow input of unique loginid and password pairs for a single host session, a range of host sessions, or all host sessions for a specific IVR application.
2. IVR Designer, Voice@Work, or Script Builder
3. Store each loginid and password pair in an encrypted file, using the RC4 128 bit Key Encryption Algorithm. Create the encrypted file, if it doesn't already exist.
NOTE: Due to United States Export Laws, the encryption used may be RC4 56 bit Key Encryption Algorithm, based on the Country the Cleo Host Interface product is used in.
4. Allow modification of the loginid and password pair for each Host Session that already exists in the encrypted file.
5. Optionally, use the same password for all Host Sessions.
6. Optionally, allow the modification of just the password portion of a loginid, password pair for a Host Session.
7. Optionally, display the LOGINIDS, only, for an application.
8. Optionally, validate the password according to custom requirements.

Cleo Encrypted Password User Guide

9. Log error messages to the Avaya Master LOG, so that the Avaya “display messages” command can be used by the System Administrator to report any Host Password Encryption Utility errors.

Installation

Avaya IR R1.1/R1.2/R1.3

Prerequisites

Before the Host Login ID Import Utility or Password Encryption Utility can be installed the following software must be installed and configured on an Avaya IR, system having a connection to a 3270-mainframe host, using SNA 3270 or TN3270 protocol.

Cleo Host Interface for SNA

Cleo Host Dip Package

Csnahdip - cleo Csnahdip V2.5 Package

Cleo SNA Software Package – Digi Sync, Token Ring, or Ethernet

Cleosna64 - Cleo SNA communications software Version 6.0.7.15

Cleo Host Interface for TCP/IP

Cleo Host Dip Package

Ctnhdip - cleo Ctnhdip V2.5 Package

Cleo TN3270 Software Package

cleotn - cleo TN3270(E) client package Version 6.0.7.16

Installation from CPIO Image

1. Login as *root*.
2. Stop the Voice System
stop_vs [wait for this step to complete; it will take several minutes]
3. If the "/export/cleo" directory does not already exist, create the directory to contain the Cleo Host Interface Extensions Software.
cd /export
mkdir cleo
chmod 777 cleo
4. After downloading and unzipping the CPIO image of the Cleo Host Interface Extensions binary Software, move the resulting file(CleoEIR25cpio.Z or CleoEIIR25cpio.Z - see note below) to the Avaya IR system and place it in the /export/cleo directory, and uncompress the file.
cd /export/cleo
uncompress CleoEIR25cpio.Z
 or
uncompress CleoEIIR25cpio.Z

NOTE: Due to United States Export Laws, the encryption used may be RC4 56 bit key encryption algorithm, based on the Country the Cleo Host Interface product is used in. In that case, use the CleoEIIR25cpio.Z file instead of the Domestic version of the software in the CleoEIR25cpio.Z file.

5. Use the following command to move the Cleo Host Interface Extensions Software from the CleoEIR25cpio file or the CleoEIIR25cpio file.
cpio -ivBdumc < CleoEIR25cpio
 or
cpio -ivBdumc < CleoEIIR25cpio

At the prompt enter the following command:

```
# pkgadd -d /export/maverick/vsdipE
```

You will be prompted to enter the packages you wish to install.
Press **ENTER** to specify all.

NOTE: Due to United States Export Laws, the encryption used may be RC4 56 bit key encryption algorithm, based on the Country the Cleo Host Interface product is used in. In that case, the pkgadd command to use is
pkgadd -d /export/maverick/vsdipEI

6. Next you will install the 16 byte RC4 Encryption Key to use for this system. You will be prompted twice to enter the key, in order to verify the Encryption Key.

Cleo Encrypted Password User Guide

```
# /vs/bin/ag/cleokey
```

Please Enter the 16 Byte RC4 Encryption Key:

Please Enter the 16 Byte RC4 Encryption Key:

NOTE: If the Encryption Key needs to be changed or re-entered, you can do so by running the program:

```
/vs/bin/ag/cleokey
```

The program will prompt for the 16 Byte RC4 Encryption Key twice, as it does at Installation Time.

If you change the 16 Byte RC4 Encryption Key, you will need to remove all existing application's encryption files(/vs/trans/applname.pwenc) and encrypt them again, using the hlogidimport/hpwencrypt/hpwupdate utilities.

NOTE: Due to United States Export Laws, the encryption used may be RC4 56 bit key encryption algorithm, based on the Country the Cleo Host Interface product is used in. In that case only 7 bytes are used for the Encryption Key, and the prompts and messages will call for 7 bytes instead of 16 bytes.

7. Next you will install the license. See *Instructions for Installing the License*.

Installation from CD

1. Login as *root*.
2. Stop the Voice System
stop_vs [wait for this step to complete; it will take several minutes]
3. Insert, into the CD ROM drive, the CD labeled
Cleo Host Interface Extensions
Domestic Distribution
for Avaya IR R1.1/R1.2
V2.5

NOTE: Due to United States Export Laws, the encryption used may be RC4 56 bit key encryption algorithm, based on the Country the Cleo Host Interface product is used in. In that case, insert, into the CD ROM drive, the CD labeled
Cleo Host Interface Extensions
International Distribution
for Avaya IR R1.1/R1.2
V2.5

4. At the prompt enter the following command:
pkgadd -d /cdrom/cdrom0/vsdipE
You will be prompted to enter the packages you wish to install.
Press **ENTER** to specify all.

NOTE: Due to United States Export Laws, the encryption used may be RC4 56 bit key encryption algorithm, based on the Country the Cleo Host Interface product is used in. In that case, the pkgadd command to use is
pkgadd -d /cdrom/cdrom0/vsdipEI

5. Next you will install the 16 byte RC4 Encryption Key to use for this system. You will be prompted twice to enter the key, in order to verify the Encryption Key.
/vs/bin/ag/cleokey

Please Enter the 16 Byte RC4 Encryption Key:
Please Enter the 16 Byte RC4 Encryption Key:
NOTE: If the Encryption Key needs to be changed or re-entered,
you can do so by running the program:
/vs/bin/ag/cleokey

The program will prompt for the 16 Byte RC4 Encryption Key twice,
as it does at Installation Time.
If you change the 16 Byte RC4 Encryption Key, you will need to
remove all existing application's encryption
files(/vs/trans/applname.pwenc) and encrypt them again, using the
hlogidimport/hpwencrypt/hpwupdate utilities.

Cleo Encrypted Password User Guide

NOTE: Due to United States Export Laws, the encryption used may be RC4 56 bit key encryption algorithm, based on the Country the Cleo Host Interface product is used in. In that case only 7 bytes are used for the Encryption Key, and the prompts and messages will call for 7 bytes instead of 16 bytes.

6. Next you will install the license. See *Instructions for Installing the License*.

Getting Started

Obtain & Register A License Key

Contact Cleo Sales to obtain and register a License Key for the Cleo Host Interface Extensions Package (vsdipE or vsdipEI) optional Password Encryption Extension Feature.

Instructions for Installing the License

1. You will need to contact Cleo Communications to Obtain a License Key for the Password Encryption Extension Feature, that is part of the **vsdipE** or **vsdipEI** Software package. You will need to provide your Avaya IR System Name to Cleo and the Cleo serial number of your system. The License Key can be supplied as a text file in addition to a text string.

To obtain your Cleo serial number, please run the command

```
# /vs/bin/ag/cleoserial -r
```

If your system does not have a Cleo serial number, please call Cleo Communications to obtain a Cleo 6 digit Serial Number and then write it to your system by running the command

```
# /vs/bin/ag/cleoserial -w nnnnnn
```

Where: nnnnnn is the Cleo 6 digit serial number

2. Obtain the Avaya IR System Name by entering the following command:

```
# uname -n
```

The System Name will be output.

3. To license the **vsdipE** or **vsdipEI** Software Package to enable the Password Encryption Extension Feature, enter the following command:

```
# /vs/bin/ag/cleohpwlic -f FILE
```

Where "FILE" is the full path to a text file containing the License Key for the Password Encryption Extension Feature

OR

```
# /vs/bin/ag/cleohpwlic
```

You will be prompted as follows. Please enter the correct information for both the serial number and License key prompts:

License File has not been verified:

Enter the serial number:

Enter the license key:

The Cleo Encryption Software is Properly Licensed

NOTE: If the serial number or license key are not input correctly, or are wrong, you will be prompted again, as shown above. You may be prompted up to 10 times, before the program will stop.

Cleo Encrypted Password User Guide

4. Next you will enable the Encrypted Password Feature. See *Instructions for Enabling the Encrypted Password Feature*.

Instructions for Enabling the Encrypted Password Feature

1. The Host DIP needs to be configured in order to enable the use of the Encrypted Password Feature.

2. Please enter the following command to Enable the Encrypted Password Feature:

```
# hdipconfig -E ON
```

NOTE: See Appendix A. for all the *hdipconfig* program options.

3. In order for the Host DIP to use the newly configured option, it is necessary to restart the Host Interface, by entering the following commands:

```
# stop_hi
```

```
# start_hi
```

4. If the need arises to DISABLE the Encrypted Password Feature, please enter the following command:

```
# hdipconfig -E OFF
```

5. You can now use the Encrypted Password Feature. See *Instructions for Using the Encrypted Password Feature*.

Instructions for Using the Encrypted Password Feature

Import existing Login ID's and Password.

1. In order to encrypt a current host application's LOGINID/PASSWORD entries, start by importing the current LOGINID and PASSWORD entries from the existing application's Host Maintenance File (/vs/trans/applicationname.hs).

```
# hlogidimport -a applicationname  
(See page 15 Using the Cleo Host Login Id Import Utility for more  
details.)
```

This will result in a new encrypted password file being created for the Host application (/vs/trans/applicationname.pwenc). Both the login IDs and the passwords will be encrypted in this file.

NOTE: The import function only imports the login IDs and passwords from the existing host maintenance script (<application name>.hs) file. It does not modify the host maintenance script.

To change encrypted Login ID and password pairs

2. In order to change the Encrypted LOGINID and PASSWORD entries for a Host application, use the **hpwencrypt** command.

(See page 17 *Using the Cleo Host Password Encryption Utility* for more details)

- a. The **hpwencrypt** command requires the OLD PASSWORD to be input, in order to change a password. If you have different passwords for each of the separate login ID, you will need to know the value(s) of each of the OLD PASSWORD(s).
- b. If you want to encrypt the existing LOGINIDs and PASSWORDs, then you can run the following command, where you will be prompted for the OLD PASSWORD and NEW PASSWORD, twice, for each session of application **test**:

```
# hpwencrypt -a test -l
```

The **hpwencrypt** command will encrypt the existing LOGINIDs, when the "-l" option is used and prompt for each OLD PASSWORD and NEW PASSWORD, twice.

NOTE: The hpwencrypt function only modifies the login IDs and passwords in the encrypted password file on the IVR system. It does not modify login IDs or passwords on the mainframe system.

Cleo Encrypted Password User Guide

Establish a single Password for all Login IDs

3. If you want to use one PASSWORD for all LOGINIDs, and, the current Host application has a different PASSWORD defined for each LOGINID, it is suggested that you use IVR Designer, Voice@Work, or Script Builder to modify the Host Maintenance script to use 1 PASSWORD. Then you will be able to use the **hpwencrypt** command to encrypt all the LOGINID and PASSWORD entries with 1 command. For example for Host Application **test** with current PASSWORD **ibm1**, to encrypt all the LOGINIDs and keep the single PASSWORD the same:

```
# hpwencrypt -a test -l -p ibm1 ibm1 ibm1
```

The **hpwencrypt** command will encrypt the existing LOGINIDs, when the **"-l"** option is used and allows for the use of a single password(given the application has a single password in its' Host Maintenance file) to be given with the **"-p oldpassword newpassword newpassword"** option.

Using The Cleo Host Login Id Import Utility

The Login ID Import Utility is invoked from the command line as follows:

```
> hlogidimport -a <app> [-f]
```

where -f is optional.

Parameters

-a <appl>

REQUIRED ARGUMENTS.

<appl> an IVR Designer, Voice@Work, or Script Builder Application name.

-f

If “-f” present, continue on and overwrite the current encrypted password file(/vs/trans/appl.pwenc), if it already exists. DO NOT PROMPT, to continue on or not.

Return Codes

RETURN CODES, when invoking hlogidimport from a Unix “system” command are:

Value	Description
0	The “hlogidimport” command completed successfully.
1	Usage error - Required arguments, -a <appl>, not supplied.
2	Usage error – Illegal argument specified
3	Application specified does not exist.
4	There are NO loginid, password pairs defined in the Application’s Host Maintenance Script File(/vs/trans/appl.hs).
5	I/O error reading the Application’s Host Maintenance Script File.
6	I/O error writing the encrypted password file(/vs/trans/appl.pwenc)
7	Error reading Encryption key
8	Another user is currently running hlogidimport or hpwencrypt for this Application.
12	The Cleo Encryption Software Serial #/License KEY is INVALID.

Examples

(NOTE: User input shown as BOLD ITALICS. Program output shown as BOLD)

1. Create an initial encrypted password file for IVR Designer Application “CLEOTEST”.

Use a single password for each LOGINID for 24 Avaya IR Host Sessions.

Be prompted for the password.

Do not be prompted for each LOGINID.

```
hlogidimport -a CLEOTEST
```

```
24 LOGINIDS were assigned NULL PASSWORDs for application CLEOTEST
```

```
hpwencrypt -a CLEOTEST -s all -p -l
```

```
Enter the old password: ENTER KEY
```

(since there is a NULL password,
just type an ENTER KEY)

```
Enter the new password:
```

(type in password followed by
ENTER KEY – nothing echoed)

```
Verify the new password:
```

(type in password again followed by
ENTER KEY – nothing echoed)

2. Create an initial encrypted password file for Script Builder Application “BANK1”.

Use a single password for each LOGINID for 96 Avaya IR Host Sessions.

Be prompted for the password.

Do not be prompted for each LOGINID.

Display the LOGINIDs in the encrypted password file.

```
hlogidimport -a BANK1
```

```
96 LOGINIDS were assigned NULL PASSWORDs for application BANK1
```

```
hpwencrypt -a BANK1 -s all -p -l
```

```
Enter the old password: ENTER KEY
```

```
Enter the new password:
```

(type in the new password – it’s not echoed)

```
Verify the new password:
```

(type in the new password – it’s not echoed)

```
hpwencrypt -a BANK1 -d
```

```
SESS 0      UID100
```

```
SESS 1      UID101
```

```
...
```

```
SESS 95     UID195
```

Using The Cleo Host Password Encryption Utility

The Password Encryption Utility is invoked from the command line as follows:

```
> hpwencrypt -a <appl> -s <sessions> [-p [oldpassword password password]] [-l] [-d]
```

where -f is optional.

Parameters

- a <appl>** REQUIRED ARGUMENTS.
<appl> an IVR Designer, Voice@Work, or Script Builder Application name.
- s <indexrange>** REQUIRED ARGUMENTS.
a single Index (n) into the Application's encrypted password file
a single range of Indices (x-y) into the Application's encrypted password file
comma separated indices (a,b,c,d) into the Application's encrypted password file
all – use all of the entries in the Application's encrypted password file
- p** OPTIONAL ARGUMENT.
If “-p” is present, then use 1 PASSWORD for all Host Session loginids.
If “-p” is present without following text string passwords, then the old password and the new password(entered twice) will be prompted for.
- p oldpassword password password** OPTIONAL ARGUMENTS.
If “-p” is present then use 1 PASSWORD for all Host Session loginids.
If “-p string string string” is present, then after successfully entering the “oldpassword” use the Specified Text Strings(password), given they are identical, as the PASSWORD for all Avaya IR Host Session loginids.
- l** OPTIONAL ARGUMENT.
If “-l” is present, then DO NOT PROMPT for loginids.
Use the loginids currently in the encrypted password file.
- d** Display the LOGINIDs, only, in the Application's encrypted password file. Only requires the -a <appl> argument. Optionally can also use the -s argument to display a range of LOGINIDs instead of the default of “all” of the LOGINIDs.

Return Codes

RETURN CODES, when invoking hlogidimport from a Unix “system” command are:

Value	Description
0	The “hpwencrypt” command completed successfully.
1	Usage error – Required arguments, -a <appl> -s <sessions>,not supplied
2	Usage error – Illegal argument specified
3	Application specified does not exist
4	Usage error – LU range specified is illegal(eg. not ascending range, range > max range value(128 V6-V7, 254 V8, R9), range not numeric, and not “all”
5	There is NO loginid, password pair defined in the Application’s encrypted password file(/vs/trans/appl.pwenc) for the specified session and the –l option is specified.
6	I/O error writing the Application’s encrypted password file (/vs/trans/appl.pwenc)
7	I/O error reading the Application’s encrypted password file (/vs/trans/appl.pwenc)
8	Another user is currently running hlogidimport or hpwencrypt for this application.
9	Old Password does not match current password(can be from command line or input from user in prompt mode after 3 failed attempts)
10	New Passwords DO NOT MATCH(can be from command line or input from user in prompt mode after 3 failed attempts)
11	Invalid New Password(didn't pass VALIDATE test)
12	Cleo ENCRYPT Feature is NOT LICENSED PROPERLY

Examples

(NOTE: User input shown as BOLD ITALICS. Program output shown as BOLD)

1. **Modify the LOGINID and PASSWORD for Script Builder Application “BANK1” for sessions 0 and 1, but keep the same LOGINID for session 31, only change the PASSWORD for session 31.**

hpwencrypt -a CLEOTEST -s 0-1,31

Enter the loginid for session 0: UID100 : *NID99*

Enter the old password for session 0: (type in the old password – it’s not echoed)

Enter the new password for session 0: (type in the new password – it’s not echoed)

Verify the new password for session 0: (type in the new password – it’s not echoed)

Enter the loginid for session 1: UID101 : *GID400*

Enter the old password for session 1: (type in the old password – it’s not echoed)

Enter the new password for session 1: (type in the new password – it’s not echoed)

Verify the new password for session 1: (type in the new password – it’s not echoed)

Enter the loginid for session 31: UID131 : *ENTER KEY* (typing just the ENTER KEY retains the original LOGINID)

Enter the old password for session 31: (type in the old password – it’s not echoed)

Enter the new password for session 31: (type in the new password – it’s not echoed)

Verify the new password for session 31: (type in the new password – it’s not echoed)

2. **CHANGE the PASSWORD for all sessions of IVR Designer Application “CLEOTEST”, but do not change the LOGINID.**

hpwencrypt -a CLEOTEST -s all -p -l

Enter the old password: (type in the old password – it’s not echoed)

Enter the new password: (type in the new password – it’s not echoed)

Verify the new password: (type in the new password – it’s not echoed)

3. **ONLY CHANGE the PASSWORD for all sessions of Script Builder Application “BANK1”.**

Enter the OLD password and NEW passwords on the command line, instead of being prompted. This could be used by a “C” program doing a UNIX “system” command.

hpwencrypt -a BANK1 -s all -p passwordold yg78#&4Bup yg78#&4Bup

Understanding the Avaya Master LOG Messages Report for the Cleo Host Loginid Import and the Cleo Host Password Encryption Utilities

MESSAGES

<u>MESSAGE NUMBER</u>	<u>MESSAGE MEANING</u>
HIMP001	hlogidimport Usage error, Must supply at least -a <appl>
HIMP002	hlogidimport Usage error, illegal arg[s] supplied
HIMP003	hlogidimport application <appl> does not Exist
HIMP004	hlogidimport No loginid, password pairs in application's host maintenance file(.hs)
HIMP005	hlogidimport Error opening application's Host Maintenance File(.hs)
HIMP006	hlogidimport I/O Error Writing Encrypted Password File
HIMP007	hlogidimport Can't overwrite existing Encrypted Password File
HIMP008	hlogidimport The <appl> Application Encrypted Password File is being processed by another hlogidimport or hpwencrypt command
HIMP012	hlogidimport The Cleo Encryption Software Serial #/License KEY is INVALID
HPWE001	hpwencrypt Usage error, Must supply at least [1] -a appl -d or [2] -a appl -s sessions
HPWE002	hpwencrypt Usage error, illegal arg[s] supplied
HPWE003	hpwencrypt application <appl> does not Exist
HPWE004	hpwencrypt (can be 1 of following) Non-numeric number in session specification Value out of range in session specification Syntax error in session specification Range limits not in ascending order in session specification Inalid session Specification
HPWE005	hpwencrypt The Password Encryption File appl.pwenc Has no Loginids defined and the option to use existing Loginids has been chosen
HPWE006	hpwencrypt Error Writing Encrypted Password File
HPWE007	hpwencrypt Error Reading Encrypted Password File
HPWE008	hpwencrypt The <appl> Application Encrypted Password File is being processed by another

HPWE009

**hlogidimport or hpwencrypt command
hpwencrypt Failed to input Correct Old
Password**

HPWE010

hpwencrypt New Passwords Do Not Match

HPWE011

hpwencrypt New Password is INVALID

HPWE012

**hpwencrypt The Cleo Encryption Software
Serial #/License KEY is INVALID**

EXAMPLE of AVAYA MASTER LOG MESSAGES

disp messages 10

```
Tue Nov 12 03:00:03 2002          hlogidimport
ADMIN001  -- -- --- root PROC_ID(pid) PROC_NAME=hlogidimport
          `hlogidimport -a appl' HIMP008 The <appl> Application
          Encrypted Password File is being processed by another
          hlogidimport or hpwencrypt command

Tue Nov 12 03:00:03 2002          ICK
ICK009   -- -- --- /var/adm/wtmpx (4014252) reduced to 372000 bytes.

Tue Nov 12 03:01:03 2002          ICK
ICK009   -- -- --- /var/adm/wtmp (388476) reduced to 36000 bytes.

Tue Nov 12 03:02:03 2002          hlogidimport
ADMIN001  -- -- --- root PROC_ID(pid) PROC_NAME=hlogidimport
          `hlogidimport' HIMP001 Usage error, Must supply at least
          -a <appl>

Tue Nov 12 03:03:03 2002          hlogidimport
ADMIN001  -- -- --- root PROC_ID(pid) PROC_NAME=hlogidimport
          `hlogidimport -a appl' HIMP004 No loginid, password pairs
          in application's host maintenance file(.hs)

Tue Nov 12 03:00:04 2002          hpwencrypt
ADMIN001  -- -- --- root PROC_ID(pid) PROC_NAME=hpwencrypt
          `hpwencrypt -a appl -d' HPWE008 The <appl> Application
          Encrypted Password File is being processed by another
          hlogidimport or hpwencrypt command

Tue Nov 12 03:00:05 2002          ICK
ICK009   -- -- --- /var/adm/wtmpx (4014252) reduced to 372000 bytes.

Tue Nov 12 03:01:06 2002          ICK
ICK009   -- -- --- /var/adm/wtmp (388476) reduced to 36000 bytes.

Tue Nov 12 03:02:07 2002          hpwencrypt
ADMIN001  -- -- --- root PROC_ID(pid) PROC_NAME=hpwencrypt
          `hpwencrypt' HPWE001 Usage Error, Must supply at least
          [1]-a appl -d or [2] -a appl -s sessions

Tue Nov 12 03:03:08 2002          hpwencrypt
ADMIN001  -- -- --- root PROC_ID(pid) PROC_NAME=hpwencrypt
          `hpwencrypt -a newapp -s 0' HPWE005 The Password
          Encryption File -newpp.pwenc- Has no Loginids defined and the
          option to use existing Loginids has been chosen
```

Trouble Shooting

Symptoms:

When invoking either the “**hlogidimport**” or “**hpwencrypt**” commands you see
License file has not been verified:
Enter the serial number:

Possible Causes:

The **cleohpw** or **cleohpwI** Software License has never been set.
The **system name** has been changed.
The **/vs/data/.cleoencrypt.lic** file has been deleted or corrupted since
initial licensing was completed.

Solution:

**Run the licensing program again, and enter the serial number and
License key:**
`/vs/bin/ag/cleohpwlic`

Symptoms:

An application that uses 1 Encrypted Password, needs to have its
Password changed, and you do **NOT KNOW THE OLD PASSWORD**.

Possible Causes:

Operator Memory Error.

Solution:

**Look up the old PASSWORD that is in the application’s Host
Maintenance file, given it was 1 password for all sessions.
Or use IVR Designer, Voice@Work, or Script Builder to change the
application’s PASSWORD in the Host Maintenance file.
Delete the application’s Encrypted Password File.**
`rm /vs/trans/applname.pwenc`
**Run hlogidimport and then hpwencrypt to create a new encrypted passwor
File.**
`hlogidimport -a appl`
`hpwencrypt -a appl -s all -l -p oldpassword newpasswd newpasswd`

Symptoms:

You have an application that was using a different unencrypted password for each
session. You want to change the application to use 1 password for all sessions
And use encrypted passwords.

Solution:

**Use IVR Designer, Voice@Work, or Script Builder and change the Password
for each session to be 1 password. This will create a new Host Maintenance
file(/vs/trans/appl.hs). Now use hlogidimport and hpwencrypt to create the
new encrypted password file. For example: if you changed the password to
FORGOT and want to change the password to NEWPASS**
`hlogidimport -a appl`
`hpwencrypt -a appl -s all -l -p FORGOT NEWPASS NEWPASS`

Symptoms:

When invoking either the **“hlogidimport”** or **“hpwencrypt”** Commands you get an **errno 13**.

Possible Causes:

You are not logged in or su'd to **“root”**.

Solution:

Login or su to “root”.

APPENDIX A.

The *hdipconfig* program is used to set/unset Host DIP configuration parameters for the MOD2-5, the Encrypted Password, and NLS(National Language Support) Features. The syntax of the command is as follows:

```
# hdipconfig [-M ON|OFF ] [-E ON|OFF] [-T ON|OFF] [TRANSTABLE]
```

-M - Model 2-5 Feature

ON - Enable Model 2-5 Feature

OFF - Disable Model 2-5 Feature

-E - Encrypted Password Feature

ON - Enable Encrypted Password Feature

OFF - Disable Encrypted Password Feature

-T - NLS Feature

ON - Enable NLS Feature

OFF - Disable NLS Feature

TRANSTABLE

An Optional EBCDIC/ASCII translation table.

TTDEFAULT - Default Translation Table US English.

TTBLANKS - Convert non US English characters to Blanks

TTHYPHENS - Convert non US English characters to Hyphens

TT1025_88595 - Cryllic Russian Character Translation

Using IBM 1025 EBCDIC and ISO 8859_5 ASCII

TT875_88597 - Greek Character Translation

Using IBM 875 EBCDIC and ISO 8859_7 ASCII

Cleo Encrypted Password User Guide

Copyright Acknowledgements

This product utilizes binary libraries for RC4 encryption written and copyrighted by Eric Young (eay@cryptsoft.com).