Rocket®

MultiValue University2015

# D3 Security – Whole File Encryption

# Lab Guide

**Developed by**
**D3 MVU Team**

# Lab Overview

## Abstract

The purpose of this lab is to demonstrate the use of Whole File Encryption. This is data encryption at rest. The data is automatically encrypted when sent to storage/disc and automatically decrypted when retrieved by D3. This helps protect your system against data theft in the event that access is gained to the storage through some means other than D3. This lab will guide the administrator through how to encrypt and decrypt a file, as well as showing the data in encrypted form by using several low level commands.

## About the Lab Environment

The lab environment uses the following:

D3 10.1 Linux or D3 9.2 Windows

## Lab Overview

- Time estimate: 45 minutes
- There are four sections to this lab:
  - Section 1: Encrypting files
  - Section 2: Viewing the data in encrypted form
  - Section 3: Encrypted data and the **`t-dump`** command
  - Section 4: Encrypted data and the **`save`** command

This lab used a controlled environment at MV University. The following exercises can be done in your own environment but you must use caution. Know what the command does before you execute it.

# Exercise 1: Encrypting files

## Purpose of the Exercise

This exercise will show you how to both create an encrypted file and encrypt an existing file.

## After this exercise you will be able to:

- Create new encrypted files
- Encrypt existing files

## Exercise Instructions

Perform the following steps:

__ 1. Log in to D3.

a. Do one of the following:

- On Linux, from the shell, enter **d3**.
- On Windows, Telnet to localhost.

b. Respond to the promps as shown below:

```
user id: dm
master dictionary: dm
```

__ 2. Create an account in which to work.

a. From the command prompt, enter the following:

```
create-account WFE
```

b. Press <Enter> eight times to go through the eight configurable options displayed. A message will be displayed indicating that the account has been created.

c. Log to the account as follows:

```
to WFE
```

__ 3. Create two files.

- The first file is a regular, non-encrypted file.

```
create-file test 1 1
```

- The second file is created as an encrypted file.

```
create-file test2 1 1 (e
```

__ 4. Display the file defining items.

a. List the files.

```
list-files (f
```

Notice the file defining item flags in the "mod" column of the "data-name". The non-encrypted file shows only the number "1", while the encrypted file shows "1de1".

__ 5. Encrypt the non-encrypted file.

If desired, this step may be done later. This will allow seeing both an encrypted and non-encrypted file throughout the lab. After completing the lab, return here, encrypt the file, and repeat the remainder of the exercises to see that the data is now encrypted.

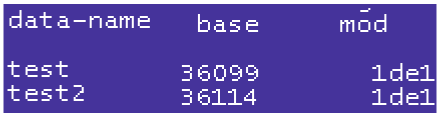
a. Enter the following command to encrypt the file:

```
encrypt-file test
```

d. List the files:

```
list-files (f
```

Notice the file defining item flags in the "mod" column of the "data-name". Both files are encrypted and both show **1de1**.



```
data-name      base       mod

test           36099      1de1
test2          36114      1de1
```

__ 6. Add an item to each file.

a. Use the method of your choice to add an item to each file. The Update Processor is used in this example:

```
u test i01
```

e. A message indicating that this is a new item will be displayed, followed by a "01" on the next line. Enter some text following the "01". For example:

```
This is my secret data.
```

f. Save the item by pressing:

```
^XF
```

g. Repeat those steps with the "test2" file.

Exercise 1 summary: Creating an encrypted file and encrypting existing files.

**End of Exercise 1**

# Exercise 2: Viewing the data in encrypted form

## Purpose of the Exercise

This exercise will show you how to view the data in encrypted form.

## After this exercise you will be able to:

- VME: Use the **`dump`** command to view VME data in encrypted form
- FSI: Use the FSI Monitor Debugger to view FSI data in encrypted form

## Exercise Instructions

Perform the following steps:

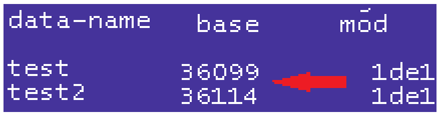
__ 1. Displaying data in its encrypted form in the VME.

This applies to D3 Linux accounts and VME accounts in D3 Windows

a. Look up the base of the data level of each of the two files.

```
list-files (f
```

Note the number in the "base" column for each of the two data levels in the "data-name" column.



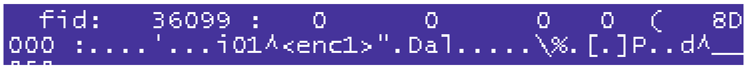
```
data-name     base      mod

test         36099      1de1
test2        36114      1de1
```

h. Dump each of those frames. Substitute the base values from your **`list-files`** report:

```
dump 36099
dump 36114
```

You will see something like the following for each of the frames:



```
  fid:   36099 :   0       0       0   0  (   8D
000 :....'...i01^<enc1>".Dal.....\%.[.]P..d^___
```

i. Notice that the item-id **`i01`** is still visible, but the item body is gibberish. This is how the data is written to storage. When accessed via D3, such as from AQL, BASIC, the MVSP APIs, etc., it is decrypted on the fly. For example, entering the following command will display the data in non-encrypted form:

```
ct test i01
```

__ 2. Displaying data in its encrypted form in the FSI.

This applies to FSI accounts on D3 Windows.

a. Enter the FSI Monitor Debugger:

```
debug
```

**md**

j. When prompted for a password, enter:

**support**

You should now be at a ">" prompt.

k. Open the account. A message will be displayed showing the current database:

**od WFE**

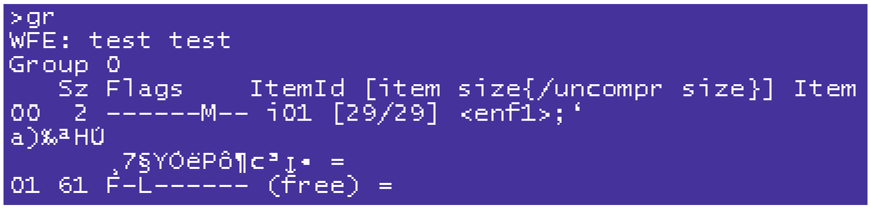
l. Open the file. Some information about the file will be displayed:

**o test**

m. Display the group in the file:

**gr**

You will see something like the following:



```
>gr
WFE: test test
Group 0
   Sz Flags    ItemId [item size{/uncompr size}] Item
00  2 ------M-- i01 [29/29] <enf1>;‘
a)‰ªHÚ
       ¸7§YÒëPô¶c³I• =
01 61 F-L------- (free) =
```

Notice that the item-id **i01** is still visible, but the item body is gibberish. This is how the data is written to storage. When accessed via D3, such as from TCL, BASIC, the MVSP APIs, etc., it is decrypted on the fly.

n. Either press enter a few times until you return to the ">" prompt or enter:

**/q**

o. This may be repeated for the other file:

**o test2**

**gr**

**/q**

p. Press **g** to go twice. Once from the ">" prompt, and then at the "!" prompt.

i. Entering the following command will display the data in non-encrypted form:

**ct test i01**

Exercise 2 summary: Viewing data in encrypted form using the **dump** command in the VME and the FSI Monitor Debugger in the FSI.

**End of Exercise 2**

# Exercise 3: Encrypted data and the t-dump command

## Purpose of the Exercise

This exercise demonstrates saving data in non-encrypted form.

## After this exercise you will be able to:

- Use the **`t-dump`** command to dump data in non-encrypted form
- Use the **`t-read`** command to read the non-encrypted data

## Exercise Instructions

Perform the following steps:

__ 1. Setup to a device to which to dump the data.

a. Enter the following command:

```
set-device
```

b. Enter the number corresponding to the “Pseudo0.D3P” device:

```
2
```

A message will be displayed indicating that the device has been assigned.

__ 2. Dump the data to storage.

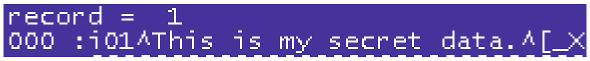
a. Rewind to the start of storage and dump the data:

```
t-rew
t-dump test
```

__ 3. Confirm that the data was written to storage in non-encrypted form.

a. Enter the following commands:

```
t-rew
t-read
```



```
record =  1
000 :i01^This is my secret data.^[_X
```

b. Notice that the item body appears in clear text. In this text, the bullet needs to be removed and the text should align with the 2 commands above. Tried to reformat myself, but couldn’t figure out how to correct.

__ 4. Detach from the storage.

```
t-det
```

__ 5. This exercise may be repeated for the “test2” file.

Exercise 3 summary: Writing the data to storage in non-encrypted form.

**End of Exercise 3**

# Exercise 4: Encrypted data and the save command

## Purpose of the Exercise

This exercise demonstrates saving data in encrypted form.

**Warning:** This only applies to D3 Linux and VME accounts on D3 Windows. FSI accounts on D3 Windows are never encrypted by the save command. This includes commands based on the save command, such as "account-save" and "file-save".

## After this exercise you will be able to:

- Use the save command to dump data in encrypted form.
- Use the t-read command to confirm the data is encrypted.

## Exercise Instructions

Perform the following steps:

__ 1. Setup to a device to which to save the data

c. Enter the following command.

```
set-device
```

d. Enter the number corresponding to the "Pseudo0.D3P" device.

```
2
```

A message will be displayed indicating that the device has been assigned.

__ 2. Save the account to storage

e. "Rewind" to the start of storage and dump the data.

```
t-rew
save (fit
```

f. When prompted for a label, press enter.

g. When prompted for the account name, enter

```
WFE
```

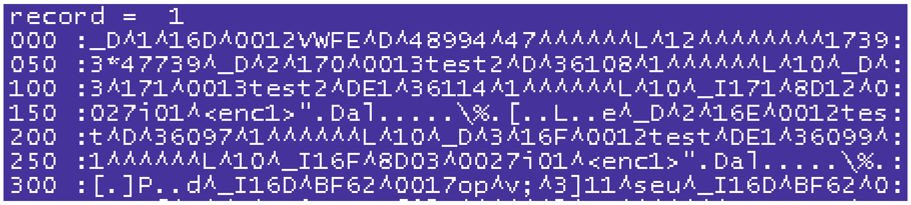
__ 3. Confirm that the data was written to storage in encrypted form

h. Enter the following commands. Note that "t-read" is entered three times.

```
t-rew
t-read
t-read
```

**t-read**

Notice that the item bodies from both "test" and "test2" remain encrypted on the backup. In this snapshot the encrypted items appear on the lines starting with "150" and "250".



```
record =  1
000 :_D^1^16D^0012VWFE^D^48994^47^^^^^^L^12^^^^^^^^^1739:
050 :3*47739^_D^2^170^0013test2^D^36108^1^^^^^^L^10^_D^:
100 :3^171^0013test2^DE1^36114^1^^^^^^L^10^_I171^8D12^0:
150 :027i01^<enc1>".Dal.....\%.[..L..e^_D^2^16E^0012tes:
200 :t^D^36097^1^^^^^^L^10^_D^3^16F^0012test^DE1^36099^:
250 :1^^^^^^L^10^_I16F^8D03^0027i01^<enc1>".Dal.....\%.:
300 :[.]P..d^_I16D^BF62^0017op^v;^3]11^seu^_I16D^BF62^0:
```

__ 4. Exit from the "t-read" command and detach from the storage

**^X**

**t-det**

Exercise 4 summary: Writing the data to storage in encrypted form.

**End of Exercise 4**