Config\_File\_Encryption\_Test Case

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 0.1 | 2008-4-10 | Zhao Haihui | Initial draft |
| 0.2 | 2008-6-26 | Zhao haihui | Add case according to 3.0r3 change |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 1. Introduction

Because our HiveAPs can be used as MPs, which are very easy to be stolen, and also our HiveOS is linux based system, which is easy to be attack to know the file systems stored in the flash. To make our HiveAPs more secure, the config file should be encrypted.

The key for encryption now in this version will be stored in the HiveOS,just like what we have done for encrypting the passwords in the cli cmds. Later the key will be stored in a security chip which is a hardware part. The encryption/descryption method is suggested to be AES-CBC.

Only the config file in flash needs to be encrypted. The config files in the memory or pushed from HiveManager or shown on the console do not need to be encrypted.

To make the original config file in plain text can also be read by new version of the HiveOS, a file header including a special field needs to be prefixed for the new encrypted config file. The special field called magiv number is used to distinguish the new encrypted file and the old plain text file.

**2. Test Topologies**

**3. Test Points and Strategies**

- Check which config files be encrypted in shell

- Check if current config be encrypted in shell

- After save config from server to current, check if corresponding config file be crypted in shell

- After save config from server to bootstrap, check if corresponding config file be encrypted in shell

- Download config from HM to current, check if corresponding config file be encrypted in shell

- Download config from HM to bootstrap, check if corresponding config file be encrypted in shell

- If exist backup config, check if corresponding backup config file be encrypted in shell

- Check if encrypted config file can be shown on the console

- Create some configurations in cli wizard , save and apply, check if corresponding config file be encrypted

- Check if config file which exist in memory be encrypted

- Downgrade image to previous image(exclude config encryption), check config on the console and config file in shell

- Save invalid config file (image) to current

- Change encrypted config file in shell to see how it handle

- Upload encrypted current config or bootstrap config to server

# 4. Software Tools Requirements

# 5. Hardware Requirements

# 6. Test Schedule

# 7. Test Case

## Case ID Ft\_Config\_File\_Encryption\_1

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_1 |
| Priority | High |
| Description | Check which config file be encrypted |
| Pre-condition | All config file exist(include configure1, configure2, bootstrap) |
| Test procedure | 1. Login AP enter shell , open directory /f/etc( or show system file flash-etc xxx) 2. Check which config file be encrypted   *AH-000180:/home/admin# cd /f/etc/*  *AH-000180:/f/etc# ls*  *ah\_rdf\_config configure1 ssh\_host\_dsa\_key.pub*  *ahtbconfig configure2 ssh\_host\_rsa\_key*  *bootstrap err\_messages ssh\_host\_rsa\_key.pub*  *configure-control ssh\_host\_dsa\_key*  *AH-000180:/f/etc# cat configure1*  *AH-000180:/f/etc# cat configure2*  *AH-000180:/f/etc# cat bootstrap* |
| Expectant result | configure1, configure2, bootstrap file be encrypted |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_2

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_2 |
| Priority | High |
| Description | Check if current config be encrypted in shell |
| Pre-condition | Exist current config |
| Test procedure | 1. Login AP 2. Check current config by CLI   *AH-000180#show config current*  *hive testhive*  *interface mgt0 hive testhive*  *ssid testssid*  *interface wifi0 ssid testssid*  *console timeout 0*  *console page 100*   1. Check which config file is current config by \_show configuration control   *AH-000180#\_show configuration control*  *system startup configuration: 1*  *config after reboot: 1*  *backup configuration: 0*  *last failed : -1*  *num: 0, valid: 1, name: /f/etc/configure1*  *num: 1, valid: 1, name: /f/etc/configure2*  *num: 2, valid: 1, name: /f/etc/bootstrap*  *num: 3, valid: 1, name: /opt/ah/etc/configure*   1. Enter shell, in directory /f/etc, check if corresponding config file be encrypted   *AH-000180:/f/etc# cat configure2* |
| Expectant result | Current config be encrypted |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_3

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_3 |
| Priority | High |
| Description | After save config from server to current, check if corresponding config file be crypted in shell |
| Pre-condition | AP connect a server, exist valid config file in server |
| Test procedure | 1. Login AP 2. Save config from tftp server to current   *AH-000180#save config tftp://10.190.0.9:testconfig current*  *Do you really want to save config to current configuration?(Y/N)y*  *AH-000180#show config current*  *hive testhive*  *interface mgt0 hive testhive*  *ssid testssid*  *ssid testssid security protocol-suite wpa-auto-psk ascii-key testtest*  *interface wifi0 ssid testssid*  *console timeout 0*  *console page 100*   1. Check which config file is current config by \_show configuration control 2. Enter shell, in directory /f/etc, check if corresponding config file be encrypted |
| Expectant result | Current config file be encrypted |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_4

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_4 |
| Priority | High |
| Description | After save config from server to bootstrap, check if corresponding config file be encrypted in shell |
| Pre-condition | AP connect a server, exist valid config file in server |
| Test procedure | 1. Login AP 2. Save config from tftp server to bootstrap   *AH-000180#save config tftp://10.190.0.9:testconfig bootstrap*  *Do you really want to download config to bootstrap configuration?(Y/N)y*  *AH-000180#show config bootstrap*  *hive testhive*  *interface mgt0 hive testhive*  *ssid testssid*  *ssid testssid security protocol-suite wpa-auto-psk ascii-key testtest*  *interface wifi0 ssid testssid*  *console timeout 0*  *console page 100*   1. Enter shell, in directory /f/etc, check if corresponding config file be encrypted   *AH-000180:/f/etc# cat bootstrap* |
| Expectant result | Bootstrap config file be encrypted |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_5

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_5 |
| Priority | High |
| Description | Download config from HM to current, check if corresponding config file be encrypted in shell |
| Pre-condition | AP connect a HM |
| Test procedure | 1. Login HM 2. Select a managed HiveAP and download complete config 3. Login this AP, check if current config is downloaded by HM 4. Check which config file is current config by \_show configuration control 5. Enter shell, in directory /f/etc, check if corresponding config file be encrypted |
| Expectant result | Config file be encrypted |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_6

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_6 |
| Priority | High |
| Description | Download config from HM to bootstrap, check if corresponding config file be encrypted in shell |
| Pre-condition | AP connect a HM |
| Test procedure | 1. Login HM 2. Select a managed AP and download bootstrap config 3. Login AP, check if bootstrap config be downloaded 4. Enter shell, in directory /f/etc, check if corresponding   config file be encrypted |
| Expectant result | Config file be encrypted |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_7

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_7 |
| Priority | High |
| Description | Check if backup config be encrypted |
| Pre-condition | AP connect a server, exist valid config file in server |
| Test procedure | 1. Loing AP 2. Create some configurations and save config 3. Save config from tftp server to current and reboot immediately 4. After reboot, login AP again 5. Check if backup config exist by show config backup 6. Check which config file is backup config file by \_show configuration control 7. Enter shell, in directory /f/etc, check if corresponding config file be encrypted |
| Expectant result | Backup config file be encrypted |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_8

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_8 |
| Priority | High |
| Description | Check if encrypted config file can be shown on the console |
| Pre-condition | Exist current config, backup config and bootstrap config, which encrypted in shell |
| Test procedure | 1. Login AP 2. Check if current config, backup config, bootstrap config be encrypted in shell 3. Exit shell, check if these config files can be shown on the console |
| Expectant result | These config can be shown on the console, which not be encrypted on the console |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_9

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_9 |
| Priority | High |
| Description | Create some configurations in cli wizard , save and apply, check if corresponding config file be encrypted |
| Pre-condition | Reset config bootstrap config |
| Test procedure | 1. Login AP 2. Reset config enter cli wizard 3. Create some configurations in cli wizard, save and apply 4. After reboot, login AP again 5. Check if current config exist 6. Check which config file is current config by \_show configuration control 7. Enter shell, in directory /f/etc, check if corresponding config file be encrypted |
| Expectant result | Config file be encrypted |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_10

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_10 |
| Priority | Low |
| Description | Check if config file which exist in memory be encrypted |
| Pre-condition | AP connect a HM |
| Test procedure | 1. Login AP, enter shell directory /tmp, check config file 2. Login HM 3. Select a managed AP and download complete config 4. While downloading, check if temporary config be encrypted (/tmp/ui\_conf\_tmp.\*) |
| Expectant result | Config file which in the memory not be encrypted |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_11

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_11 |
| Priority | Low |
| Description | Downgrade image to previous image(exclude config encryption), check config show on the console and config file in shell |
| Pre-condition | Exist current config, backup config, bootstrap config |
| Test procedure | 1. Login AP 2. Check current config, backup config and bootstrap config by cli 3. Enter shell, check if these config files be encrypted 4. Downgrade image to previous image (no config file encryption) and reboot 5. After reboot, check these config |
| Expectant result | Encrypted config file could not be decrypted |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_12

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_12 |
| Priority | Low |
| Description | Save invalid config file (image) to current , check if suggest error |
| Pre-condition | AP connect a server, exist image file |
| Test procedure | 1. Login AP 2. Save image to current 3. Check if suggest error |
| Expectant result | Suggest “save config failed” |
| Test result | *AH-000180#save config tftp://10.190.0.9:/eng/3.0r3/eap6628-ah3.0.3-07021741.img current*  *Do you really want to save config to current configuration?(Y/N)y*  *ERROR: save configuration failed!* |

## Case ID Ft\_Config\_File\_Encryption\_13

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_13 |
| Priority | Low |
| Description | Change encrypted config file in shell to see how it handle |
| Pre-condition | Exist encrypted current config |
| Test procedure | 1. Login AP 2. Check current config by cli 3. Enter shell, change encrypted config file 4. Exit shell, check current config |
| Expectant result | After change checksum, fail to decrypt, current config could not be shown, will suggest error |
| Test result | *AH-001920#show config current*  *ERROR: The current configuration file /f/etc/configure2 appears to be corrupted. Verification of the file checksum failed.* |

## Case ID Ft\_Config\_File\_Encryption\_14

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_14 |
| Priority | High |
| Description | Upload encrypted current config or bootstrap config to server |
| Pre-condition | Exist encrypted current config and bootstrap config |
| Test procedure | 1. Login AP 2. Check current config and bootstrap config by cli 3. Enter shell, check if corresponding config file be encrypted 4. Exit shell, upload current config or bootstrap config to server 5. Check config file in server |
| Expectant result | Can see decrypted config in server |
| Test result |  |

## 3.0r3 enhancement:

Add a command “show config current info:

Show encrypt information stored in the header of configuration file. Include Magic number, Length of data, Checksum and File version … If the file is corrupted, can let user show the corrupt file.

## Case ID Ft\_Config\_File\_Encryption\_15

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_15 |
| Priority | High |
| Description | When current config file is fine, check config information |
| Pre-condition | Exist current config |
| Test procedure | 1. Login AP 2. Create some configurations and save config 3. Check current config by cli 4. Check current config information by cli, verify if include Magic number, Length of data, Checksum and File version,etc 5. Check encrypted config file in shell |
| Expectant result |  |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_16

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_16 |
| Priority | Middle |
| Description | When current config file is corrupt, verify if can show corrupt config file |
| Pre-condition | Current config file is corrupt(change config file header or content in shell) |
| Test procedure | 1. Login AP 2. Check current config   *AH-000180#show config current*  *ERROR: The current configuration file /f/etc/configure1 appears to be corrupted. Verification of the file checksum failed.*   1. Check current config information   *AH-000180#show config current info*  *Do you want to print the corrupt file? (Y/N)n*   1. Verify if suggest print corrupt config file 2. Type “Y” 3. Check current file information, verify if print out corrupt config   *The info of the current configuration file:*  *Magic number: 0x01ff55aa*  *IV: 0xd035be756f15586a6cace3d05eda086c*  *File size: 500*  *Checksum: 0xde6512ded9f292fa09dd9ec964799c5c*  *Wrong checksum: 0xfe1a37eb4c182a050f5acb0510189dce*  *File version: 2*  *Paddings: 4*  *Reserved: 0x0000*  *Data of configuratin file:*  *00000000 686f7374 6e616d65 2041482d 30303031 hostname AH-0001*  *00000016 38300a73 6e6d7020 6c6f6361 74696f6e 80.snmp location*  *00000032 2068616e 677a686f 752d6165 726f6869 hangzho u-aerohi*  *00000048 76650a61 646d696e 20737570 65727573 ve.admin superus*  *00000064 65722074 65737474 65737474 65737474 er testt esttestt*  *00000080 65737474 65737420 70617373 776f7264 esttest password*  *00000096 20497343 4f663370 6f596953 536e7270 IsCOf3p oYiSSnrp*  *00000112 66cc9408 598b19c7 b32f5642 c8107631 f...Y... ./VB..v1*  *00000128 5efe3e67 f9dd501f 2ab1aa54 a44c6f4c ^.>g..P. \*..T.LoL*  *00000144 4e0cf155 7d498deb 5b0e91e1 1a0bcce4 N..U}I.. [.......*  *00000160 6231cbc3 d76d936a cf5b51ab b4593c52 b1...m.j .[Q..Y<R*  *00000176 279bfdb9 42908cd5 0d24b4ce 92ba0799 '...B... .$......*  *00000192 cacbee4f 822581c6 5837a48a 1e0b405f ...O.%.. X7....@\_*  *00000208 a7e628d7 2e2a55eb f04e34e5 b5c9545e ..(..\*U. .N4...T^*  *00000224 30ba9ae1 c8974231 7fa0d763 7665422c 0.....B1 ...cveB,*  *00000240 49ac8dc0 69d9bec2 ab09fb3e 66ac6fec I...i... ...>f.o.*  *00000256 173f7439 b0edb6a2 69189307 e79f4381 .?t9.... i.....C.*  *00000272 e461e29b 7b1f71f6 3f88d771 b623fd8f .a..{.q. ?..q.#..*  *00000288 1155595d 2f4ac447 2c3e8a14 50dd8221 .UY]/J.G ,>..P..!*  *00000304 a001ba09 a164b2dd e713f866 e7622467 .....d.. ...f.b$g*  *00000320 9714b210 9632f004 ac035fad bbb968df .....2.. ..\_...h.*  *00000336 45bd197b a75ce66e 42d33bfe aed69e4b E..{.\.n B.;....K*  *00000352 5ad46adb cae2f966 cb901a9c 5f669f2f Z.j....f ....\_f./*  *00000368 fc348efe 011960b9 15f0c4ae 681f1605 .4....`. ....h...*  *00000384 dc24095f 07e9cd5d adf74856 cfcdee18 .$.\_...] ..HV....*  *00000400 a412e5ec fe2d1e4a 66602a7e 99e4b569 .....-.J f`\*~...i*  *00000416 4123c134 c8ef9865 d40f68b5 a7dc4e3e A#.4...e ..h...N>*  *00000432 03d78862 5ff0b585 3a7b28e7 cc17353d ...b\_... :{(...5=*  *00000448 9d29c5dd e47b7a3e 344a3548 000005b0 .)...{z> 4J5H....*  *00000464 00000681 0fc36048 0fc36048 000005c0 ......`H ..`H....* |
| Expectant result | Current config is corrupt and could not show normally  When show config current info, will suggest “Do you want to print the corrupt file?”  Type “y”, will show current config info include Magic number, Length of data, Checksum and File version,etc  and print out corrupt config |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_17

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_17 |
| Priority | Middle |
| Description | When type “n”, verify will not print corrupt file |
| Pre-condition | Current config file is corrupt |
| Test procedure | 1. Login AP 2. Check current config 3. Check current config information 4. Verify if suggest print corrupt config file 5. Type “n” 6. Check current file information, verify if print out corrupt config |
| Expectant result | Current config is corrupt and could not show normally  When show config current info, will suggest “Do you want to print the corrupt file?”  Type “n”, will show current config info include Magic number, Length of data, Checksum and File version,etc  but not print out corrupt config |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_18

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_18 |
| Priority | Accept |
| Description | Don’t change current config and save config, IV will change and other parameter don’t change when show config current info |
| Pre-condition | Exist current config |
| Test procedure | 1. Login AP 2. Check current config 3. Check current config info 4. Save config 5. Check current config info |
| Expectant result | After save config, IV will change and other parameter don’t change |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_19

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_19 |
| Priority | Accept |
| Description | Once current config change , IV and checksum will both change when show config current info |
| Pre-condition | Exist current config |
| Test procedure | 1. Login AP 2. Check current config 3. Check current config info 4. Create some configurations and save config (or save config to current from tftp server) 5. Check current config 6. Check current config info |
| Expectant result | After current config change, IV and checksum change |
| Test result |  |

## Case ID Ft\_Config\_File\_Encryption\_20

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_20 |
| Priority | Middle |
| Description | Save a fine config to current and substitute corrupt config, verify if suggest “Do you want to print the corrupt file?” when show config current info |
| Pre-condition | Current config is corrupt |
| Test procedure | 1. Login AP 2. Check current config 3. Check current config info 4. Create some configurations and save config(or save config to current from tftp server) 5. Check current config 6. Check current config info |
| Expectant result | After save fine config to substitute corrupt config, don’t suggest “Do you want to print the corrupt file?” |
| Test result |  |

**Upgrade Test:**

## Case ID Ft\_Config\_File\_Encryption\_21

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_21 |
| Priority | High |
| Description | Upgrade image of AP from 2.1or 3.0b2(no config file encryption) to 3.0r1(encrypted version1), check all config |
| Pre-condition | AP with version 2.1 or 3.0b2  Exist current config, backup config and bootstrap config in AP (upload config from HM or by CLI) |
| Test procedure | 1. Login AP   2. Check version and config by CLI( *hiveap20-2.1r5.img.S*)  *Version: HiveOS 2.1r5*  *Build host: Sirius*  *Build time: Wed Apr 23 00:19:39 PDT 2008*  *Build by: buildmaster*  *Platform: HiveAP20\_ag*  *Uptime: 0 weeks, 0 days, 0 hours, 10 minutes, 12 seconds*  3.Upgrade image to 3.0r1and reboot  *upgrade to: hiveap20-3.0r1.img.S*  4.After reboot, login AP again   1. Check AP version and all config by CLI 2. Check if all config file be encrypted in shell |
| Expectant result | All config can be shown normally by CLI |
| Test result | After upgrade image from 2.1r5 to 3.0r1:  All config can be shown normally  Previous config still not be encrypted  If save new config to current or bootstrap, new config will be encrypted |

## Case ID Ft\_Config\_File\_Encryption\_22

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_22 |
| Priority | High |
| Description | Upgrade image of AP from 2.1(no config file encryption) to 3.0r3(encrypted version2), check all config |
| Pre-condition | AP with version 2.1  Exist current config, backup config and bootstrap config in AP (upload config from HM or by CLI) |
| Test procedure | 1. Login AP 2. Check version and all config by CLI(hiveap20-2.1r5.img.S) 3. Upgrade image to 3.0r3 and reboot (eap6628-ah3.0.3-07021741.img) 4. After reboot, login AP again 5. Check AP version and all config by CLI 6. Check if all config file be encrypted in shell 7. Check current config info |
| Expectant result | All config can be shown normally by CLI |
| Test result | After upgrade image from 2.1r5 to 3.0r3:  All config can be shown normally  Previous config still not be encrypted  After save new config to current or bootstrap, new config will be encrypted, encrypted config file version show 2 |

## Case ID Ft\_Config\_File\_Encryption\_23

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_23 |
| Priority | High |
| Description | Upgrade image of AP from 3.0r1(encrypted version 1) to 3.0r3 (encrypted version 2), check all config |
| Pre-condition | AP with version 3.0r1  Exist current config, backup config and bootstrap config in AP (upload config from HM or by CLI) |
| Test procedure | 1. Login AP 2. Check version and all config by CLI (hiveap20-3.0r1.img.S) 3. Upgrade image to 3.0r3 and reboot(eap6628-ah3.0.3-07021741.img) 4. After reboot, login AP again 5. Check AP version and all config by CLI 6. Check if all config file be encrypted in shell 7. Check current config info |
| Expectant result | All config can be shown normally by CLI |
| Test result | After upgrade image:  All config can be shown by CLI  All config file still be encrypted  Current config file version show 1, after save config, version show 2 |

## Case ID Ft\_Config\_File\_Encryption\_24

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_24 |
| Priority | High |
| Description | Upgrade image of AP from 3.0r2 to 3.0r3, check all config |
| Pre-condition | AP with version 3.0r2  Exist current config, backup config and bootstrap config in AP (upload config from HM or by CLI) |
| Test procedure | 1. Login AP 2. Check version and all config by CLI(hiveap20-3.0r2.img.S) 3. Upgrade image to 3.0r3 and reboot(eap6628-ah3.0.3-07021741.img) 4. After reboot, login AP again 5. Check AP version and all config by CLI 6. Check if all config file be encrypted in shell 7. Check current config info |
| Expectant result | All config can be shown normally by CLI |
| Test result | After upgrade image from 3.0r2 to 3.0r3:  All config can be shown normally  All config file still be encrypted  Current config file version show 2 |

**Negative Test:**

## Case ID Ft\_Config\_File\_Encryption\_25

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_25 |
| Priority | Low |
| Description | Change the checksum field of the encrypted file by manual, check if it will fail the decryption process and what message will be shown out |
| Pre-condition | Exist current config |
| Test procedure | 1. Login AP 2. Check current config 3. Check current config info 4. Change the checksum field of the encrypted file by manual 5. Check if current config can be shown correctly 6. Check current config info 7. Check if print out error log |
| Expectant result | After change checksum, fail to decrypt, current config could not be shown, will suggest error |
| Test result | *Before change checksum:*  *AH-001920#show config current info*  *The info of the current configuration file:*  *Magic number: 0x01ff55aa*  *IV: 0x151e6cc061b5021959bdd1071af8ad29*  *File size: 116*  *Checksum: 0x7c43da2d0811b2b4cfec4bccc94b7514*  *File version: 2*  *Paddings: 15*  *Reserved: 0x0000*  *After change checksum:*  *AH-001920#show config current*  *ERROR: The current configuration file /f/etc/configure1 appears to be corrupted. Verification of the file checksum failed.*  *AH-001920#show conf*  *AH-001920#show config c*  *AH-001920#show config current info*  *AH-001920#show config current info*  *Do you want to print the corrupt file? (Y/N)y*  *The info of the current configuration file:*  *Magic number: 0x01ff55aa*  *IV: 0x151e6cc061b5021959bdd1071af8ad29*  *File size: 116*  *Checksum: 0x7c111111111111111111111111111111*  *Wrong checksum: 0x7c43da2d0811b2b4cfec4bccc94b7514*  *File version: 2*  *Paddings: 15*  *Reserved: 0x0000*  *Data of configuratin file:*  *00000000 68697665 20207a68 68686976 650a696e hive zh hhive.in*  *00000016 74657266 61636520 206d6774 30206869 terface mgt0 hi*  *00000032 76652020 7a686868 6976650a 636f6e73 ve zhhh ive.cons*  *00000048 6f6c6520 70616765 20203130 300a636f ole page 100.co*  *00000064 6e736f6c 65207469 6d656f75 74202030 nsole ti meout 0*  *00000080 0a000000 00000000 00000000 00000000 ........ ........*  *AH-001920#show log bu | in warn*  *1970-01-01 00:25:31 warn checksum error when decrypt the file /f/etc/configur e1*  *1970-01-01 00:18:49 warn checksum error when decrypt the file /f/etc/configur e1*  *1970-01-01 00:15:40 warn checksum error when decrypt the file /f/etc/configur e1* |

## Case ID Ft\_Config\_File\_Encryption\_26

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_26 |
| Priority | Low |
| Description | Change the IV field of the encrypted file by manual, check if will fail the decryption process and what message will be shown out |
| Pre-condition | Exist current config |
| Test procedure | 1. Login AP 2. Check current config 3. Check current config info 4. Change the IVfield of the encrypted file by manual 5. Check if current config can be shown correctly 6. Check current config info 7. Check if print out log |
| Expectant result | After change IV, fail to decrypt, current config could not be shown, will suggest error |
| Test result | *Before change IV:*  *AH-001920#show config current info*  *The info of the current configuration file:*  *Magic number: 0x01ff55aa*  *IV: 0xedb05450dfc98db35a86e9109d013de5*  *File size: 116*  *Checksum: 0x7c43da2d0811b2b4cfec4bccc94b7514*  *File version: 2*  *Paddings: 15*  *Reserved: 0x0000*  *after change IV:*  *AH-001920:/f/etc# tftp -m binary 10.155.30.9 -c put configure1*  *AH-001920:/f/etc# tftp -m binary 10.155.30.9 -c get configure1*  *AH-001920:/f/etc# exit*  *Welcome back to CLI console!*  *AH-001920#show con*  *AH-001920#show conf*  *AH-001920#show config c*  *AH-001920#show config current*  *ERROR: The current configuration file /f/etc/configure1 appears to be corrupted. Verification of the file checksum failed.*  *AH-001920#show config current info*  *AH-001920#show config current info*  *Do you want to print the corrupt file? (Y/N)y*  *The info of the current configuration file:*  *Magic number: 0x01ff55aa*  *IV: 0xadbd2332323322332323232321111115*  *File size: 116*  *Checksum: 0x7c43da2d0811b2b4cfec4bccc94b7514*  *Wrong checksum: 0x0793af694c35c08d2f6f77d1856911e7*  *File version: 2*  *Paddings: 15*  *Reserved: 0x0000*  *Data of configuratin file:*  *00000000 28640107 cddad5e8 11cda345 d91a459e (d...... ...E..E.*  *00000016 74657266 61636520 206d6774 30206869 terface mgt0 hi*  *00000032 76652020 7a686868 6976650a 636f6e73 ve zhhh ive.cons*  *00000048 6f6c6520 70616765 20203130 300a636f ole page 100.co*  *00000064 6e736f6c 65207469 6d656f75 74202030 nsole ti meout 0*  *00000080 0a000000 00000000 00000000 00000000 ........ ........*  *AH-001920#show log bu | in warn*  *1970-01-01 00:25:31 warn checksum error when decrypt the file /f/etc/configur e1*  *1970-01-01 00:18:49 warn checksum error when decrypt the file /f/etc/configur e1*  *1970-01-01 00:15:40 warn checksum error when decrypt the file /f/etc/configur e1* |

## Case ID Ft\_Config\_File\_Encryption\_27

|  |  |
| --- | --- |
| Case ID | Ft\_Config\_File\_Encryption\_27 |
| Priority | Low |
| Description | Change the length of data field of the encrypted file by manual, check if will fail the decryption process and what message will be shown out |
| Pre-condition | Exist current config |
| Test procedure | 1. Login AP 2. Check current config 3. Check current config info 4. Change the length of data field of the encrypted file by manual 5. Check if current config can be shown correctly 6. Check current config info 7. Check if print out log |
| Expectant result | After change length of data, fail to decrypt, current config could not be shown, will suggest error |
| Test result | *Before change data of length:*  *AH-001920#show config current*  *hive zhhhive*  *interface mgt0 hive zhhhive*  *console page 100*  *console timeout 0*  *AH-001920#show config current info*  *The info of the current configuration file:*  *Magic number: 0x01ff55aa*  *IV: 0xb0779b32c44c87ee17781497421ea288*  *File size: 116*  *Checksum: 0x7c43da2d0811b2b4cfec4bccc94b7514*  *File version: 2*  *Paddings: 15*  *Reserved: 0x0000*  *after change IV:* |