Alif Security Toolkit

V1.104.0

ALIF
SEMICONDUCTOR

ALIF
SEMICONDUCTOR

ALIF
SEMICONDUCTOR

NOTE:

app

Example:

```
$ ./maintenance
[INFO] COM8 open Serial port success
[INFO] baud rate 55000

Available options:

 1 - Device Control
 2 - Device Information
 3 - MRAM
 4 - Utilities
 5 - Setting capabilities
 6 - ROM

Select an option (Enter to exit): |
```

```
$ python3 <tool-name>.py
```

```
$ <tool-name>
$ ./<tool-name>
```

```
$ cd <release-location>
$ updateSystemPackage
```

```
Burning: System Package in MRAM
Selected Device:
Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B4

Connecting to the target device...
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM7 open Serial port success
Bootloader stage: SERAM
[INFO] Detected Device:
Part# AE722F80F55D5LS - Rev: B4
- MRAM Base Address: 0x80580000
Maintenance Mode = Enabled
Authenticate Image:  True
Verify Certificate
Signature File:  alif\SP-AE722F80F55D5LS-rev-b4-dev.bin.sign
Download Image
alif\SP-AE722F80F55D5LS-rev-b4-dev.bin[####################]100%: 270368/270368 bytes
Verify Image
Done
       5.82 seconds

Authenticate Image:  True
Verify Certificate
Signature File:  alif\offset-58-rev-b4-dev.bin.sign
Download Image
alif\offset-58-rev-b4-dev.bin   [####################]100%: 16/16 bytes
Verify Image
Done
       0.02 seconds
```

```
$ cd <release-location>
  edit build/config/app-cfg.json and add new binaries images

$ app-gen-toc

(Or use below command to use a different configuration)

$ app-gen-toc -f build/config/app-myfile.json

$ app-write-mram
```

COM7 - Tera Term VT

File Edit Setup Control Window Help

```
SEROM v1.96.0 0x0000B400

SES B4 v1.104.0 Feb 18 2025 17:31:48
[SES] No ATOC
[SES] STOC DEVICE ok
[SES] No LF XTAL

[SES] SERAM bank 0x0 is valid and booted
[SES] STOC ok
[SES] M55-HE booted from address 0x58000000
[SES] LCS=1
[SES] FC:Rgn
0:2 7:0 8:0 9:0 13:0 13:1 13:2

+----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
|   Name   |  CPU   | Store Addr |  Obj Addr  | Dest Addr  | Boot Addr  |   Size   |  Version  |  Flags | Time (ms)|
+----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
|   DEVICE |  CM0+  | 0x805C1EC0 | 0x805C14C0 | ---------- | ---------- |      340 |      1.0.0| u V    |    15.83 |
| * SERAM0 |  CM0+  | ---------- | 0x000000C0 | ---------- | ---------- |    90360 |    1.104.0| ------ |     0.00 |
|   SERAM1 |  CM0+  | ---------- | 0x00020AC0 | ---------- | ---------- |    90360 |    1.104.0| ------ |     0.00 |
+----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
Legend: (u)(C)ompressed,(L)oaded,(V)erified,(s)kipped verification,(B)ooted,(E)ncrypted,(D)eferred

[SES] SE frequency is 100.85 MHz
```

```
[SES] No ATOC
[SES] System partition address  0x80580000
[SES] STOC DEVICE ok
[SES] No LF XTAL
[SES] STOC ok
```

```
[SES] STOC ok
[SES] ATOC ok
```

ALIF
SEMICONDUCTOR

Firewall exception from FC13, caused by Master ID 0x11 at address 0x80580000, transaction properties 0x00020000

```
[WARNING] ATOC firewall configuration skipped: FC:11 Rgn:1 error=3
```

Error	Definition	Description

```
[SES] No ATOC
[SES] System partition address  0x80580000
[SES] STOC DEVICE ok
[SES] No LF XTAL
[SES] STOC ok
[SES] M55-HE booted from address 0x58000000
[SES] LCS=1
[SES] FC:Rgn
0:2 7:1 8:1 9:1 13:0 13:1 13:2
```

```
$ cd <release-location>
$ app-write-mram
```

```
$ cd <release-location>
$ app-gen-toc -f build/config/app-cfg.json
$ app-write-mram
```

NOTE

```
app-gen-toc
```

only

```
IF ATOC is present
   Process ATOC and Boot
ELSE
  IF MTOC is present
    Process MTOC and Boot
ELSE
  IF (0x80000000 and 0x80000004 has valid $SP and $PC)
      ReleaseM55_HE
  ELSE
      Load STOC Debug stub (if present)
```

-
-

-
-

NOTE

ALIF
SEMICONDUCTOR

```
[SES] System TOC address 0x80580000
[DEV] Change Set
+------------+------------+------------+
|   Address  |    Mask    |    Value   |
+------------+------------+------------+
| 0x08000004 | 0xFFFFFFFF | 0xDEADBEEF |
| 0x0800000C | 0x0000FFFF | 0xDEADBEEF |
| 0x08000010 | 0xFFFFFFFF | 0x0000C0DE |
| 0x08000008 | 0xFFFFFFFF | 0x0000CAFE |
+------------+------------+------------+
[DEV] Wounding Data: 0x00C03FFB
[SES] System      partition processed (0x00000000) BL_STATUS_OK
[DEV] Change Set
+------------+------------+------------+
|   Address  |    Mask    |    Value   |
+------------+------------+------------+
| 0x08000018 | 0xFFFF0000 | 0xDEADBEEF |
+------------+------------+------------+
[SES] Application partition processed (0x00000000) BL_STATUS_OK
```

-

Invalid address in STOC partition

```
[SES] LCS=0
[SES] System partition address  0x80580000
[DEV] Change Set
+------------+------------+------------+
|   Address  |    Mask    |    Value   |
+------------+------------+------------+
| 0x08000018 | 0xFFFFFFFF | 0xDEADBEEF |
| 0x805C14E0 | 0xFFFFFFFF | 0x0000CAFE |
[ERROR] address 805c14e0 is in STOC partition
+------------+------------+------------+
[DEV] Wounding Data: 0x00C03FFB
[SES] System      partition processed (0x00000000) BL_STATUS_OK
[SES] Application partition processed (0x00000000) BL_STATUS_OK
```


-
-

```
 updateSystemPackage.py
Burning: System Package in MRAM
Selected Device:
Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B4

Connecting to the target device...
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[ERROR] openSerial could not open port 'COM7': PermissionError(13, 'Access is denied.', None, 5)
[ERROR] isp openSerial failed for COM7
```

```
Available options:

1 - Hard maintenance mode
2 - Soft maintenance mode
3 - Device reset

Select an option (Enter to return): 1

[ERROR] /dev/ttyUSB0 readSerial reporting disconnected
```

```
$ ./maintenance
[ERROR] openSerial could not open port 'COM8': FileNotFoundError(2, 'The system cannot find the file specified.', None, 2)
[ERROR] isp openSerial failed for COM8
```

```
$ ./app-write-mram -d
Writing MRAM with parameters:
Device Part# E7 (AE722F80F55D5AS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- Available MRAM: 5767168 bytes
[INFO] Burning: ../build/AppTocPackage.bin 0x8057c4e0
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
COM ports detected = 2
-> COM8
-> COM9
Enter port name:
```

tools-config

Not required

build/config/app-cfg.json

AppTocPackage.bin

```
app-gen-toc -f build/config/app-cpu-stubs.json

app-write-mram -e app

app-write-mram
```

```
+----------+--------+------------+------------+------------+------------+----------+-------+--------+----------+
|   Name   |  CPU   | Store Addr |  Obj Addr  | Dest Addr  | Boot Addr  |   Size   |Version| Flags  | Time (ms)|
+----------+--------+------------+------------+------------+------------+----------+-------+--------+----------+
|   SERAM0 |  CM0+  | ---------- | 0x00000120 | ---------- | ---------- |    54976 | 1.0.0 | u s    |     0.00 |
|   SERAM1 |  CM0+  | ---------- | 0x00020B20 | ---------- | ---------- |    54976 | 1.0.0 | u s    |     0.00 |
|   DEVICE |  CM0+  | 0x805C1F20 | 0x805C1520 | ---------- | ---------- |      760 | 0.5.5 | u V    |    10.41 |
|  A32_DBG | A32_0  | 0x805C2C20 | 0x805C2220 | 0x02000000 | 0x02000000 |      644 | 1.0.0 | uLVB   |     9.69 |
|   HP_DBG | M55-HP | 0x805C38B0 | 0x805C2EB0 | 0x50000000 | 0x50000000 |     2256 | 1.0.0 | uLVB   |     9.95 |
|   HE_DBG | M55-HE | 0x805C4B80 | 0x805C4180 | 0x60000000 | 0x60000000 |     2256 | 9.9.9 | uLVB   |     9.97 |
+----------+--------+------------+------------+------------+------------+----------+-------+--------+----------+
Legend: (u)(C)ompressed,(L)oaded,(V)erified,(s)kipped verification,(B)ooted,(E)ncrypted,(D)eferred
```

- updateSystemPackage
- app-write-mram

```
SETOOLS OPTIONS CONFIGURATION


* * * * * * * * * * * * * * * * * * * * * * * *
Current configuration
 - DEVICE Family: Ensemble - Part#: E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B4
 - MRAM BURNER
     Interface:  isp
     JTAG Adapter: J-Link
* * * * * * * * * * * * * * * * * * * * * * * *

Available options:

1 - Part#
2 - Revision
3 - Interface
4 - JTAG Adapter

5 - Exit (default)

Please enter the number of your option: |
```

$ tools-config

```
Available options:

1 - Ensemble (default)

Please enter the number of your option: 1

Available options:

1 - E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM (default)
2 - E7 (AE722F80F55D5AS) - 5.5 MRAM / 13.5 SRAM
3 - E5 (AE512F80F55D5LS) - 5.5 MRAM / 13.5 SRAM
4 - E5 (AE512F80F5582AS) - 5.5 MRAM / 8.25 SRAM
5 - E5 (AE512F80F55D5AS) - 5.5 MRAM / 13.5 SRAM
6 - E5 (AE512F80F5582LS) - 5.5 MRAM / 8.25 SRAM
7 - E3 (AE302F80F55D5LE) - 5.5 MRAM / 13.5 SRAM
8 - E3 (AE302F80F5582LE) - 5.5 MRAM / 8.25 SRAM
9 - E3 (AE302F80F55D5AE) - 5.5 MRAM / 13.5 SRAM
10 - E3 (AE302F80F5582AE) - 5.5 MRAM / 8.25 SRAM
11 - E3 (AE302F80C1557LE) - 1.5 MRAM / 5.75 SRAM
12 - E3 (AE302F40C1537LE) - 1.5 MRAM / 3.75 SRAM
13 - E1 (AE101F4071542LH) - 1.5 MRAM / 4.5 SRAM

Please enter the number of your option: |
```

-
    -
    -
    -
-
    -
    -
    -

```
$ app-gen-rot (-h for help)
```

```
$ ./app-gen-rot -o
utils/key/hbk1_hash.txt
utils/key/hbk1_zeros.txt
utils/key/kce.txt
utils/key/OEMRoT.pem
utils/key/OEMRoTPublic.pem
utils/key/OEMSBContent.pem
utils/key/OEMSBContentPublic.pem
utils/key/OEMSBKey.pem
utils/key/OEMSBKeyPublic.pem
utils/key/oem_keys_pass.pwd
cert/OEMSBKey1.crt
cert/OEMSBKey2.crt
cert/SBapp-device-config.bin.crt
cert/SBm55_blink_he.bin.crt
cert/SBm55_he_power_test.bin.crt
cert/SBm55_hp_power_test.bin.crt
Please enter a new password for the keys to generate:silly
Generating APP RoT keys (to be used in Key 1 Certificate)
2023-06-28 15:53:37,367 - RSA Key Generator Utility started (Logging to build/logs/key_gen_log.log)
2023-06-28 15:53:37,724 - Private key written to: utils/key/OEMRoT.pem
2023-06-28 15:53:37,726 - Public key written to: utils/key/OEMRoTPublic.pem
2023-06-28 15:53:37,726 - Script completed successfully
Generating APP SB Key keys (to be used in Key 2 Certificate)
2023-06-28 15:53:37,727 - RSA Key Generator Utility started (Logging to build/logs/key_gen_log.log)
2023-06-28 15:53:38,200 - Private key written to: utils/key/OEMSBKey.pem
2023-06-28 15:53:38,212 - Public key written to: utils/key/OEMSBKeyPublic.pem
2023-06-28 15:53:38,213 - Script completed successfully
Generating APP SB Content keys (to be used in Content Certificates)
2023-06-28 15:53:38,214 - RSA Key Generator Utility started (Logging to build/logs/key_gen_log.log)
2023-06-28 15:53:38,446 - Private key written to: utils/key/OEMSBContent.pem
2023-06-28 15:53:38,449 - Public key written to: utils/key/OEMSBContentPublic.pem
2023-06-28 15:53:38,449 - Script completed successfully
Generating APP Hbk1
2023-06-28 15:53:38,451 - HBK Generator Utility started (Logging to build/logs/gen_hbk_log.log)
2023-06-28 15:53:38,451 - Step 1: Calculating hash
2023-06-28 15:53:38,452 - Step 2: Calculating zeros hash
2023-06-28 15:53:38,454 - Keying complete successfully
Generating gen-hbk-key [Configure]
2023-06-28 15:53:38,460 - Key Generation Tool Started (Logging to build/logs/OEMSBKey1.log)
2023-06-28 15:53:38,460 - Reading config file: utils/cfg/OEMSBKey1.cfg
2023-06-28 15:53:38,474 - Parsed Keys:
{"cert-keypair", "utils/key/OEMRoT.pem"}, {"cert-keypair-pwd", "utils/key/oem_keys_pass.pwd"}, {"HBK-Y", "1"}, {"avcounter-val", "0"}, {"next-cert-pubKey", "utils/key/OEMSBKeyPublic.pem"}, {"cert-pkg", "cert/OEMSBKey1.crt"}
2023-06-28 15:53:38,477 - Dump content of config file:
#This configuration file is for the offline-key-certificate-tool=cert-key-ubl.py=(key-certificate-generation tool -KCG).
```

```
2023-06-28 15:53:38,472 - Raw content of config file:
# This configuration file is for the offline key certificate tool cert_key_util.py (Key Certificate Generation Tool - KCGT).
#
# The available parameters in this configuration file are the following
#   â€¢ [KEY-CFG]        : Mandatory header.
#          The internal non-configurable header.
#   â€¢ cert-keypair     : Mandatory parameter.
#          The file holding the RSA keypair for signing this certificate, in PEM format.
#   â€¢ cert-keypair-pwd : Optional. If omitted the tool prompts for direct input.
#          The passphrase file for the keypair file, in .txt format.
#   â€¢ hbk-id           : Mandatory parameter. The tool is agnostic to the certificate usage, this parameter cannot be omitted.
#          The ID of the Hbk field in OTP memory that the public key of this certificate is verified against:
#             - 0: 128-bit Hbk0.
#             - 1: 128-bit Hbk1.
#             - 2: 256-bit Hbk.
#          The ROM code uses this field only if this certificate is the first certificate in:
#             - A two-level SB certificate chain.
#             - A three-level SB certificate chain.
#             - A three-level Secure Debug chain.
#   â€¢ nvcounter-val    : Mandatory parameter.
#          The NV counter value:
#             - 0..64: the ICV counter.
#             - 0..96: the OEM counter.
#             - 0..160: the full counter, if OEM and ICV are a single entity.
#          The passphrase file for the keypair file, in .txt format.
#   â€¢ next-cert-pubkey : Mandatory parameter.
#          The file holding the RSA public key for signing the next certificate in the chain, in PEM format.
#   â€¢ cert-pkg         : Mandatory parameter.
#          The key certificate package output file.
[KEY-CFG]
cert-keypair = utils/key/OEMSBKey.pem
cert-keypair-pwd = utils/key/oem_keys_pass.pwd
hbk-id = 1
nvcounter-val = 0
next-cert-pubkey = utils/key/OEMSBContentPublic.pem
cert-pkg = cert/OEMSBKey2.crt

2023-06-28 15:53:38,474 - **** Creating Key certificate ****
2023-06-28 15:53:38,482 - Write the certificate to file
2023-06-28 15:53:38,484 - **** Certificate file creation has been completed successfully ****
Generating APP SB Key 2 Certificate
2023-06-28 15:53:38,485 - Key Certificate Generation Utility started (Logging to build/logs/OEMSBKey2.log)
2023-06-28 15:53:38,486 - Parsing config file: utils/cfg/OEMSBKey2.cfg
2023-06-28 15:53:38,493 - Parsed items:
[('cert-keypair', 'utils/key/OEMSBKey.pem'), ('cert-keypair-pwd', 'utils/key/oem_keys_pass.pwd'), ('hbk-id', '1'), ('nvcounter-val', '0'), ('next-cert-pubkey', 'utils/ke
y/OEMSBContentPublic.pem'), ('cert-pkg', 'cert/OEMSBKey2.crt')]
2023-06-28 15:53:38,494 - Raw content of config file:
# This configuration file is for the offline key certificate tool cert_key_util.py (Key Certificate Generation Tool - KCGT).
#
# The available parameters in this configuration file are the following
#   â€¢ [KEY-CFG]        : Mandatory header.
#          The internal non-configurable header.
#   â€¢ cert-keypair     : Mandatory parameter.
#          The file holding the RSA keypair for signing this certificate, in PEM format.
#   â€¢ cert-keypair-pwd : Optional. If omitted the tool prompts for direct input.
#          The passphrase file for the keypair file, in .txt format.
#   â€¢ hbk-id           : Mandatory parameter. The tool is agnostic to the certificate usage, this parameter cannot be omitted.
#          The ID of the Hbk field in OTP memory that the public key of this certificate is verified against:
#             - 0: 128-bit Hbk0.
#             - 1: 128-bit Hbk1.
#             - 2: 256-bit Hbk.
#          The ROM code uses this field only if this certificate is the first certificate in:
#             - A two-level SB certificate chain.
#             - A three-level SB certificate chain.
#             - A three-level Secure Debug chain.
#   â€¢ nvcounter-val    : Mandatory parameter.
#          The NV counter value:
#             - 0..64: the ICV counter.
#             - 0..96: the OEM counter.
#             - 0..160: the full counter, if OEM and ICV are a single entity.
#          The passphrase file for the keypair file, in .txt format.
#   â€¢ next-cert-pubkey : Mandatory parameter.
#          The file holding the RSA public key for signing the next certificate in the chain, in PEM format.
#   â€¢ cert-pkg         : Mandatory parameter.
#          The key certificate package output file.
[KEY-CFG]
cert-keypair = utils/key/OEMSBKey.pem
cert-keypair-pwd = utils/key/oem_keys_pass.pwd
hbk-id = 1
nvcounter-val = 0
next-cert-pubkey = utils/key/OEMSBContentPublic.pem
cert-pkg = cert/OEMSBKey2.crt

2023-06-28 15:53:38,497 - **** Creating Key certificate ****
2023-06-28 15:53:38,505 - Write the certificate to file
2023-06-28 15:53:38,506 - **** Certificate file creation has been completed successfully ****

Check logs in build/logs/ directory
Done!
```

utils/key/ *cert/* *build/logs/*

build/config/app-cfg.json

app-cfg - Notepad

File Edit Format View Help

```
{
        "BLINK-HE": {
                "binary": "m55_blink_he.bin",
                "version" : "1.0.0",
                "cpu_id": "M55_HE",
        "loadAddress": "0x58000000",
        "flags": ["load", "boot"]
        },
        "DEVICE": {
        "binary": "app-device-config.json",
        "version" : "0.5.00"
    }
}
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

```
"IMAGE_IDENTIFIER": {
      "attribute_1": "value_1",
      "attribute_2": "value_2",
      ……————
      "attribute_n": "value_n"
}
```

```
{
   "IMAGE_1": {

   },
   "IMAGE_2": {

   },
   ……————————
   "IMAGE_N": {

   }
}
```

binary

version

loadAddress

mramAddress

flags

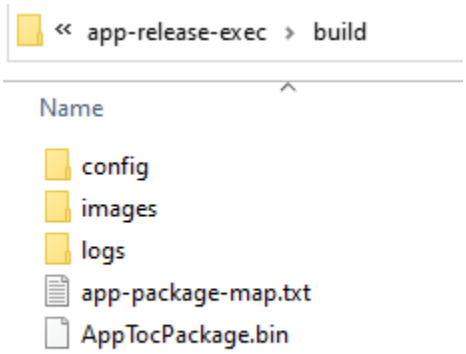
-
-
-
-
-

cpu_id

<u>Note:</u> Only one CPU_ID should be specified.

signed

disabled



Once the *app-cfg.json* file is configured as desired, we need to be sure that all declared images do exist In the *build/images/* folder.

After running the *app-gen-toc.py* tool, the **APP TOC Package** (AppTocPackage.bin) will be generated in the *build/* folder.

The *build/logs/* folder contains a log for the Generation (OEMSBContent.log file)

build/images/

```
$ app-gen-toc (-h for help)
```

```
$ ./app-gen-toc
Generating APP Package with:
Device Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- System MRAM Base Address: 0x80580000
- APP MRAM Base Address: 0x80000000
- APP MRAM Size: 5767168
- Configuration file: build/config/app-cfg.json
- Output file: build/AppTocPackage.bin

Generating Device Configuration for: app-device-config.json
Calculating APP area...
Creating Content Certificates...
2024-01-26 13:46:31,300 - Content Certificate Generation Utility started (Logging to ../build/logs/ICVSBContent.log)
2024-01-26 13:46:31,561 - Content Certificate Generation Utility started (Logging to ../build/logs/ICVSBContent.log)
Creating APP TOC Package...
Adding ATOC...
APP TOC Package size: 15104 bytes
Creating Signature...
Binary File:  ../build/AppTocPackage.bin
2024-01-26 13:46:31,809 - Content Certificate Generation Utility started (Logging to ../build/logs/ICVSBContent.log)
Content Certificate File:  build/AppTocPackage.bin.crt
Signature File:  build/AppTocPackage.bin.sign
Done!
```

app-package-map.txt

oem-package-map.txt - Notepad

File Edit Format View Help

```
* * * User managed MRAM locations* * *
0xa0000100      0x280   640     signed  a32_stub_0.bin

* * * OEM Package Start Address* * *

  - Certificates for User managed images
0xa057d670      0x690   1680    Key1/Key2 Certificates
0xa057dd00      0x370   880     SBa32_stub_0.bin.crt

  - Certificates & images for Tool managed images
0xa057e070      0x370   880     SBm55_stub_hp.bin.crt
0xa057e3e0      0x8d0   2256    m55_stub_hp.bin
0xa057ecb0      0x690   1680    Key1/Key2 Certificates
0xa057f340      0x370   880     SBm55_stub_he.bin.crt
0xa057f6b0      0x8d0   2256    m55_stub_he.bin

  - OEM TOC (Table of Content)
0xa057ff80      0x10    16      OEM TOC Header
0xa057ff90      0x20    32      OEM TOC entry for A32_0    obj_a
0xa057ffb0      0x20    32      OEM TOC entry for M55_HP   obj_a
0xa057ffd0      0x20    32      OEM TOC entry for M55_HE   obj_a
0xa057fff0      0x10    16      OEM TOC Tail

OEM Package Summary:
 - OEM Package total size: 10640 bytes
 - OEM Package Start Address: 0xa057d670
 - OEM TOC size: 128 bytes
 - OEM TOC Start Address: 0xa057ff80
 - OEM CRC32: 0xe25282ff

* * * END of OEM Package * * *
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

Start Address	Size	Name	Name

```
$ ./app-gen-toc -f build/config/app-cfg-1c.json
$ ./app-write-mram
```

•

$ app-write-mram (-h for help)

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.

C:\app-release-exec>app-write-mram.exe -h
usage: app-write-mram.exe [-h] [-d] [-b BAUDRATE] [-e ERASE] [-i IMAGES] [-a] [-m METHOD] [-S] [-s] [-x] [-p] [-nr]
                          [-V] [-v]

NVM Burner for Application TOC Package

optional arguments:
  -h, --help            show this help message and exit
  -d, --discover        COM port discovery
  -b BAUDRATE, --baudrate BAUDRATE
                        serial port baud rate
  -e ERASE, --erase ERASE
                        ERASE [APP | <start address> <size> [<pattern>] ]
  -i IMAGES, --images IMAGES
                        images list to burn into NVM ("/path/image1.bin 0x80001000 /path/image2.bin 0x80003000")
  -a, --auth_image      authenticate the image by sending its signature file
  -m METHOD, --method METHOD
                        loading method [JTAG | ISP]
  -S, --skip            write ATOC only - skip user managed images
  -s, --switch          dynamic baud rate switch toggle, default=on
  -x, --exit            exit on NAK
  -p, --pad             pad the binary if size is not multiple of 16
  -nr, --no_reset       do not reset target before operation
  -V, --version         Display Version Number
  -v, --verbose         verbosity mode

C:\app-release-exec>
```

```
$ ./app-write-mram
Writing MRAM with parameters:
Device Part# E7 (AE722F80F55D5AS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- Available MRAM: 5767168 bytes
[INFO] Burning: ../build/AppTocPackage.bin 0x8057c4e0
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM8 open Serial port success
Maintenance Mode = Enabled
Authenticate Image:  False
build\AppTocPackage.bin         [####################]100%: 15136/15136 bytes
      0.32 seconds
```

```
$ app-write-mram -a
```

```
$ ./app-write-mram
Writing MRAM with parameters:
Device Part# E7 (AE722F80F55D5AS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- Available MRAM: 5767168 bytes
[INFO] Burning: ../build/AppTocPackage.bin 0x8057c4e0
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM8 open Serial port success
Maintenance Mode = Enabled
Authenticate Image:  False
build\AppTocPackage.bin         [####################]100%: 15136/15136 bytes
      0.32 seconds
```

Enabled

Erasing all the application MRAM

```
$ app-write-mram -e app
```

```
$ ./app-write-mram -e app
Writing MRAM with parameters:
Device Part# E7 (AE722F80F55D5AS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- Available MRAM: 5767168 bytes
[INFO] Erasing: erase 0x80000000 0x580000
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM8 open Serial port success
[INFO] erase 0x80000000 5767168 (5,767,168)
```

Erasing a specific address of application MRAM

Erasing a specific address of application MRAM

```
$ ./app-write-mram -e "0x80000000 0x10"
Writing MRAM with parameters:
Device Part# E7 (AE722F80F55D5AS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- Available MRAM: 5767168 bytes
[INFO] Erasing: erase 0x80000000 0x10
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM8 open Serial port success
[INFO] erase 0x80000000 16 (16)
```

Erasing a specific address of application MRAM with a pattern

```
$ ./app-write-mram -e "0x80000000 0x10 0xa5a5a5a5"
Writing MRAM with parameters:
Device Part# E7 (AE722F80F55D5AS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- Available MRAM: 5767168 bytes
[INFO] Erasing: erase 0x80000000 0x10 0xa5a5a5a5
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM8 open Serial port success
[INFO] erase 0x80000000 16 (16)
```

Erasing a specific address of MRAM that is illegal.

```
$ ./app-write-mram -e "0x80580000 0x10"
Writing MRAM with parameters:
Device Part# E7 (AE722F80F55D5AS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- Available MRAM: 5767168 bytes
[INFO] Erasing: erase 0x80580000 0x10
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM8 open Serial port success
[INFO] erase 0x80580000 16 (16)
[ERROR] illegal address 0x80580010 (0x80580000 + 0x10)
```

ALIF
SEMICONDUCTOR

The -S option will write only the ATOC to MRAM. Any managed images to be written will be ignored.

The -s option will toggle the dynamic baud rate change when performing bulk transfer operations. By

The HFRC is not very precise, and it is possible that on some boards it runs at a quite different frequency from its nominal 76.8MHz, this may result in seeing ISP errors (such as Checksum).

The policy was changed and starting with V83 – the policy when there is no ATOC is to assume that the external crystals HFXO and LFXO are present, and to switch the device to using them, including starting the PLL and switching to it.

The app-write-mram tool, when using ISP protocol, will probe the device to get the Part# and Revision. If these parameters are different than the one configured in the tools (via tools-config tool), a Warning message will be displayed:

```
C:\Windows\System32\cmd.exe

C:\Projects\QA\DEV\firmware\setools\app-release>python3 app-write-mram.py
Writing MRAM with parameters:
Device Part# E7 (AE722F80F55D5AS) - 5.5 MRAM / 13.5 SRAM - Rev: B3
- Available MRAM: 5767168 bytes
[INFO] Burning: ../build/AppTocPackage.bin 0x8057bf50
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM12 open Serial port success
[INFO] Detected Device:
Part# AE722F80F55D5LS - Rev: B4
[WARN] ************ Part# detected is different than the one configured in tools-config tool!
[WARN] ************ Part Revision detected is different than the one configured in tools-config tool!
Maintenance Mode = Enabled
Authenticate Image:  False
Download Image
build\AppTocPackage.bin         [####################]100%: 16560/16560 bytes
Done
       0.40 seconds
```

If for any reason, the device is in SEROM Recovery mode, the app-write-mram tool will not work as it requires an SES image to be running the tool will probe the device, via ISP, to check if SEROM or SES is running. If device is in Recovery mode, then it will warn the user about this condition and exit;

```
C:\Windows\System32\cmd.exe

C:\Projects\QA\DEV\firmware\setools\app-release>python3 app-write-mram.py
Writing MRAM with parameters:
Device Part# E7 (AE722F80F55D5AS) - 5.5 MRAM / 13.5 SRAM - Rev: B3
- Available MRAM: 5767168 bytes
[INFO] Burning: ../build/AppTocPackage.bin 0x8057bf50
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM12 open Serial port success
[ERROR] The device is in RECOVERY MODE! Please use Recovery option in Maintenance Tool to recover the device!

C:\Projects\QA\DEV\firmware\setools\app-release>
```

$ updateSystemPackage

```
Burning: System Package in MRAM
Selected Device:
Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B4

Connecting to the target device...
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM7 open Serial port success
Bootloader stage: SERAM
[INFO] Detected Device:
Part# AE722F80F55D5LS - Rev: B4
- MRAM Base Address: 0x80580000
Maintenance Mode = Enabled
Authenticate Image:  True
Verify Certificate
Signature File:  alif\SP-AE722F80F55D5LS-rev-b4-dev.bin.sign
Download Image
alif\SP-AE722F80F55D5LS-rev-b4-dev.bin[####################]100%: 270368/270368 bytes
Verify Image
Done
       5.82 seconds

Authenticate Image:  True
Verify Certificate
Signature File:  alif\offset-58-rev-b4-dev.bin.sign
Download Image
alif\offset-58-rev-b4-dev.bin   [####################]100%: 16/16 bytes
Verify Image
Done
       0.02 seconds
```

Bootloader stage: SERAM

Device Revision: B0

$ updateSystemPackage -nr

```
$ updateSystemPackage -na
```

```
Burning: System Package in MRAM
Selected Device:
Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B2

Connecting to the target device...
[INFO] baud rate  55000
[INFO] dynamic baud rate change  Enabled
[INFO] COM8 open Serial port success
Bootloader stage: SERAM
[INFO] Detected Device:
Part# AE722F80F55D5LS - Rev: B4
- MRAM Base Address: 0x80580000
Connected target is not the default Revision
Do you want to set this part as default? (y/n): |
```

detected

$ maintenance (-h for help)

```
$ ./maintenance -h
usage: maintenance.exe [-h] [-b BAUDRATE] [-d] [-opt OPTION] [-V] [-v]

FUSION Maintenance Tool

optional arguments:
  -h, --help            show this help message and exit
  -b BAUDRATE, --baudrate BAUDRATE
                        serial port baud rate
  -d, --discover        COM port discovery
  -opt OPTION, --option OPTION
                        call option [sesbanner]
  -V, --version         Display Version Number
  -v, --verbose         verbosity mode
```

$ maintenance -opt <option>

```
maintenance.py --opt seshanner
SES B4 v1.101.0 Sep 27 2024 23:28:22
```

Action	Menu Groups							
	Device Control	Device Info	MRAM	Utilities	Set	ROM	SEROM	SES

```
C:\Projects\QA\DEV\firmware\setools\app-release>python3 maintenance.py
COM ports detected = 2
-> COM12
-> COM13
Enter port name:COM12
[INFO] COM12 open Serial port success
[INFO] baud rate 55000
[INFO] Connecting to target...Device connected in Recovery

Available options:

 1 - ROM
 2 - Device Information
 3 - Utilities

Select an option (Enter to exit):
```

```
Select an option (Enter to exit): 1

Available options:

1 - Hard maintenance mode
2 - Soft maintenance mode
3 - Device reset

Select an option (Enter to return):
```

Hard maintenance Mode

Soft maintenance Mode

Device Reset

```
Available options:

 1 - Get TOC info
 2 - Get SES Banner
 3 - Get CPU boot info
 4 - Device enquiry
 5 - Get revision info
 6 - Get OTP data
 7 - Get MRAM data
 8 - Get log data
 9 - Get SEROM trace data
10 - Get SERAM trace data
11 - Get power data
12 - Get clock data
```

Get Table of contents information

```
Select an option (Enter to return): 1
 +----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
 |   Name   |  CPU   | Store Addr |  Obj Addr  | Dest Addr  | Boot Addr  |   Size   |  Version  |  Flags | Time (ms)|
 +----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
 |    DEVICE|   CM0+ | 0x805c1ee0 | 0x805C14E0 | ---------- | ---------- |      404 |      0.5.0|u V     |    14.58 |
 |    SERAM0|   CM0+ | ---------- | 0x000000E0 | ---------- | ---------- |    78208 |      1.0.0|------- |     0.00 |
 |    SERAM1|   CM0+ | ---------- | 0x00020AE0 | ---------- | ---------- |    78208 |      1.0.0|------- |     0.00 |
 |    HE_DBG| M55-HE | 0x805c2a80 | 0x805C2080 | 0x58000000 | 0x58000000 |     2256 |      1.0.0|uLVB    |    14.73 |
 +----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+

Available options:
```

Legend Reference

Get SES Banner

```
Select an option (Enter to return): 2
 SES B4 v1.103.0 Dec 12 2024 20:07:29
```

NOTE:

Get CPU boot information

```
Select an option (Enter to return): 3
 +--------+------+------------+
 |  CPU   |Booted| Boot Addr  |
 +--------+------+------------+
 | A32_0  |      | ---------- |
 | A32_1  |      | ---------- |
 | M55-HP |      | ---------- |
 | M55-HE | YES  | 0x58000000 |
 +--------+------+------------+
```

Device Enquiry

```
SERAM Error =  0x0 Extended Error =  0x0 Maintenance Mode = Disabled

Available options:
```

```
Select an option (Enter to return): 4
SERAM Error =  0x0 Extended Error =  0x0 Maintenance Mode = Enabled

Available options:
```

```
Available options:

 1 - Get TOC info
 2 - Get SES Banner
 3 - Get CPU boot info
 4 - Device enquiry
 5 - Get revision info
 6 - Get OTP data
 7 - Get MRAM data
 8 - Get log data
 9 - Get SEROM trace data
10 - Get SERAM trace data
11 - Get power data
12 - Get clock data

Select an option (Enter to return): 4
SEROM Error =  0x12 (SEROM_ATOC_HEADER_STRING_INVALID)  Extended Error =  0x0 Maintenance Mode = <None>
```

Get Revision Information

Item	Meaning

Revision B4

```
Select an option (Enter to return): 5
 Source          =  SERAM
 Version         =  0xB400
 ALIF_PN         =  AE722F80F55D5LS
 HBK0            =  f049442ecc7900a838d34c31d71e62e6
 HBK1            =  00000000000000000000000000000000
 HBK_FW          =  0000000000000000000000000000000000000000
 Wounding        =  0xc1
        DFT     Disable
        Modem   Disable
        GNSS    Disable
 DCU             =  0x0
 MfgData         =  0401041500000017000000000000000000000017809f30d883003c00a000000088
        + x-loc     21
        + y-loc     4
        + Fab       UAS Global
        + Wafer ID 1
        + Year#     2024
        + Week#     23
        + Lot#      0
 LCS             =  0x1 (DM)
```

Get OTP data

```
Select an option (Enter to return): 6
Enter word addr(hex): 51
0x0051 0x0

Available options:
```

ALIF
SEMICONDUCTOR

Get trace data

```
Select an option (Enter to return): 9
*** SERAM Trace Buffer decode ***
*** Trace Header ***
[00000256]   1a1a23
[00000260] eeeeeeee
trace_total = 26
********************
  Address      Seq#      LR                  Trace Marker                          Marker Data
[00000000]      1      0x022F       Begin Reset_Handler
[00000004]      2      0x023B       Turn On System Power                          0x0000003F
[0000000c]      3      0x2D31       SE Firewall configuration
[00000010]      4      0x2D3F       HOST Firewall configuration
[00000014]      5      0x4B5D       Firewall controller ready
[00000018]      6      0x024D       Firewall initialized
[0000001c]      7      0x0257       Begin CGU clock configuration
[00000020]      8      0x0265       CGU clock configuration complete
[00000024]      9      0x0E55       SOC reset was triggered                       0x00000002
[0000002c]     10      0x0E61       SOC reset was triggered                       0x00000000
[00000034]     11      0x0EED       SOC reset was triggered
[00000038]     12      0x4D05       Begin Main
[0000003c]     13      0x2CA5       Begin CC312 initializations
[00000040]     14      0x2CD9       LCS = 0 -> CM
[00000044]     15      0x0A95       Find STOC in MRAM
[00000048]     16      0x0C73       Bank A is newer
[0000004c]     17      0x1131       Locate certificate chain
[00000050]     18      0x1183       Verify certificate chain
[00000054]     19      0x1081       Begin certificate chain verification          0x00000003
[0000005c]     20      0x1093       Verify each certificate                       0x901CC8E0
[00000064]     21      0x1093       Verify each certificate                       0x901CCC28
[0000006c]     22      0x1093       Verify each certificate                       0x901CCF70
[00000074]     23      0x10FB       End certificate chain verification
[00000078]     24      0x4B41       Load MSP Address                              0x3001FE00
[00000080]     25      0x4B23       Load JUMP Address                             0x30006CC5
[00000088]     26      0x0E2D       Jump to SERAM
```

```
Select an option (Enter to return): 10
*** SERAM Trace Buffer decode ***
*** Trace Header ***
[0x000001d8] 0x002c2c57
[0x000001dc] 0xeeeeeeee
trace_total = 44
********************
  Address      Seq#      LR                Trace Marker                          Marker Data
[00000004]      1      0x6FCF      Cold boot                                     T:     468
[0000000c]      2      0x730D      CC Lib BEGIN                                  T:    1420
[00000014]      3      0x7335      CC Lib END                                    T:    2505
[0000001c]      4      0x25CB      Firewall Static BEGIN                         T:    4032
[00000024]      5      0x2751      Firewall Static END                           T:   24973
[00000028]      6      0x275B      Firewall initialized
[00000030]      7      0xA7D7      Begin DCU configuration                       T:   26472
[00000034]      8      0xA7E5      Begin DCU configuration                       0xFFFFFFFF
[0000003c]      9      0xA7F9      Finish DCU configuration                      0xFFFFFFFF
[000000bc]     25      0xBB1D      Full trim specified                           0x00000002
[000000c4]     26      0xBB3F      Program VBAT ANA REG2                         0x000C0686
[00000110]     [illegible]  0xB2A1  Finish initializing analog GPIO values        T: [illegible]
[00000116]     [illegible]  0x7489  BANK Maintenance BEGIN                        T: [illegible]
[00000120]     [illegible]  0x7[illegible]  BANK Maintenance END                  T: [illegible]
[00000126]     [illegible]  0x7441  STOP Process BEGIN                            T: [illegible]
[00000130]     [illegible]  0x[illegible]  MSS_HP released                        T: [illegible]
[00000136]     [illegible]  0x[illegible]  SC_Prim BEGIN                          T: [illegible]
[00000140]     [illegible]  0x[illegible]  SC_Prim END                            T: [illegible]
[00000146]     [illegible]  0x[illegible]  SERAM load complete                    T: [illegible]
[0000014c]     [illegible]  0x0A6[illegible]  Read SOC_ID                         0x[illegible]
[[illegible]]  [illegible]  [illegible]  [illegible]                              [illegible]

                                                Available options:
```

Get Power data

```
Select an option (Enter to return): 11
  es0_ppu_status        0x00000000      OFF
  es1_ppu_status        0x00000008      ON
  se_ppu_status         0x00000008      ON
  fw_ppu_status         0x00000007      FUNC_RET
  systop_ppu_status     0x00000008      ON
  dbgtop_ppu_status     0x00000008      ON
  clustop_ppu_status    0x00000000      OFF
  a32_0_ppu_status      0x00000000      OFF
  a32_1_ppu_status      0x00000000      OFF
  modem_ppu_status      0x00000000      OFF
  modem_aon_status      0x00000000      OFF
  sse700_aon_status     0x00000001      ON
```

NOTE

Get Clock data

```
12 - Get clock data

Select an option (Enter to return): 12
        Clock Status:
          HFXTAL STARTED
          PLL LOCKED
          SE CLOCK: PLL
        CLK freq A32 800Mhz
        CLK freq ES0 400Mhz
        CLK freq ES1 160Mhz
        SE frequency 100.03MHz

        Registers:
        HOSTCPUCLK_CTRL : 0x00000004
        HOSTCPUCLK_DIV0 : 0x001F0000
        HOSTCPUCLK_DIV1 : 0x001F0000
        ACLK_CTRL       : 0x00000202
        ACLK_DIV0       : 0x00000000
        OSC_CTRL        : 0x00110011
        PLL_LOCK_CTRL   : 0x00000001
        PLL_CLK_SEL     : 0x00110111
        ESCLK_SEL       : 0x00000033
        CLK_ENA         : 0x11033111
        SYSTOP_CLK_DIV  : 0x00000102
        MISC_REG1       : 0x000002A4
        XO_REG1         : 0x11D08439
           xtal_cap:8  gm_pfet:16  gm_nfet:16
        PD4_CLK_SEL     : 0x00000000
        PD4_CLK_PLL     : 0x00000000
        MISC_CTRL       : 0x00001001
        DCDC_REG1       : 0x614DE693
        DCDC_REG2       : 0x8F014441
        VBAT_ANA_REG1   : 0x06479E80
resh:0     osc_rc_32k_freq_cont:0  xtal32k_en:1  xtal32k_gm_cont:15  xtal32k_cap_cont:8  bor_en:1  bor_hyst:1  bor_th
        VBAT_ANA_REG2   : 0x000C06B6
ow:1       pmubg_vref_cont:11  osc_76Mrc_cont_bit0:1  osc_76M_div_cont_fast:0  osc_76Mrc_cont:16  osc_76M_div_cont_sl
```

ALIF
SEMICONDUCTOR

```
Select an option (Enter to exit): 3

Available options:

 1 - Erase Application Mram
 2 - Fast Erase Application Mram
 3 - Fast Erase App. Mram (include NTOC)
 4 - Get MRAM info

Select an option (Enter to return):
```

Erase Application MRAM

```
Select an option (Enter to return): 1
 +----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
 |   Name   |  CPU   | Store Addr |  Obj Addr  | Dest Addr  | Boot Addr  |   Size   |  Version  |  Flags | Time (ms)|
 +----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
 |    DEVICE|   CM0+ | 0x8057cb90 | 0x8057C190 | ---------- | ---------- |      296 |      0.5.0|u V     |    15.44 |
 |    DEVICE|   CM0+ | 0x805c1ec0 | 0x805C14C0 | ---------- | ---------- |      340 |      1.0.0|u V     |    15.74 |
 |  * SERAM0|   CM0+ | ---------- | 0x000000C0 | ---------- | ---------- |    83408 |    1.101.0|u s     |     0.00 |
 |    SERAM1|   CM0+ | ---------- | 0x00020AC0 | ---------- | ---------- |    83408 |    1.101.0|------- |     0.00 |
 |  BLINK-HE| M55-HE | 0x8057d6c0 | 0x8057CCC0 | 0x58000000 | 0x58000000 |    10440 |      1.0.0|uLVB    |    16.92 |
 +----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+

Available options:
```

```
Available options:

1 - Erase Application Mram
2 - Fast Erase Application Mram
3 - Get MRAM info

Select an option (Enter to return): 1
[INFO] erasing 0x80000000 5,767,168 bytes
[INFO] Full Erase done

Available options:

1 - Erase Application Mram
2 - Fast Erase Application Mram
3 - Get MRAM info

Select an option (Enter to return):
```

```
Select an option (Enter to return): 1
 +----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
 |   Name   |  CPU   | Store Addr |  Obj Addr  | Dest Addr  | Boot Addr  |   Size   |  Version  |  Flags | Time (ms)|
 +----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
 |    DEVICE|   CM0+ | 0x805c1ec0 | 0x805C14C0 | ---------- | ---------- |      340 |      1.0.0|u V     |    15.74 |
 |  * SERAM0|   CM0+ | ---------- | 0x000000C0 | ---------- | ---------- |    83408 |    1.101.0|u s     |     0.00 |
 |    SERAM1|   CM0+ | ---------- | 0x00020AC0 | ---------- | ---------- |    83408 |    1.101.0|------- |     0.00 |
 +----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
```

Fast Erase Application MRAM

clear

Fast Erase Application MRAM (including NTOC)

Get MRAM info (MRAM Walker)

```
Available options:

1 - Erase Application Mram
2 - Fast Erase Application Mram
3 - Get MRAM info

Select an option (Enter to return): 3
 ATOC  0x8057ffc0
        + header        OEMTOC01
        + header_size   16
        + # toc entries 1
        + entry_size    32
        + version       0x1
 STOC  0x80580000
        + header        ALIFTOC1
        + header_size   48
        + # toc entries 4
        + entry_size    32
        + version       0x1
 ATOC  0x8058eca0
 ATOC  0x805af6a0
```

```
Select an option (Enter to exit): 4

Available options:

 1 - Terminal mode
 2 - Get SERAM metrics
 3 - Get ECC key
 4 - Get Firewall configuration

Select an option (Enter to return):
```

Terminal Mode

```
Select an option (Enter to return): 1
[TERMINAL] Ctrl-C to exit


SEROM v1.96.0 0x0000B400


SES B4 v1.103.0 Dec 12 2024 20:07:29
[SES] No ATOC
[SES] STOC DEVICE ok
[SES] No LF XTAL

[SES] SERAM bank 0x0 is valid and booted
[SES] STOC ok
[SES] M55-HE booted from address 0x58000000
[SES] LCS=1
[SES] FC:Rgn
0:2 7:0 8:0 9:0 13:0 13:1 13:2


+----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
|   Name   |  CPU   | Store Addr |  Obj Addr  | Dest Addr  | Boot Addr  |   Size   |  Version  |  Flags | Time (ms)|
+----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
|   DEVICE |  CM0+  | 0x805C1EC0 | 0x805C14C0 | ---------- | ---------- |      340 |      1.0.0| u V    |    15.83 |
| * SERAM0 |  CM0+  | ---------- | 0x000000C0 | ---------- | ---------- |    86196 |    1.103.0| ------ |     0.00 |
|   SERAM1 |  CM0+  | ---------- | 0x00020AC0 | ---------- | ---------- |    86196 |    1.103.0| ------ |     0.00 |
+----------+--------+------------+------------+------------+------------+----------+-----------+--------+----------+
Legend: (u)(C)ompressed,(L)oaded,(V)erified,(s)kipped verification,(B)ooted,(E)ncrypted,(D)eferred


[SES] SE frequency is 102.99 MHz
```

SES Metrics

```
Available options:

1 - Terminal mode
2 - Get SERAM metrics

Select an option (Enter to return): 2
 +-------------------------------+
 |   TaskName       | Size | Used |
 +-----------------+------+------+
 | SERAM_main_task | 1024 |  300 |
 | SERAM_uart_task | 3072 |  720 |
 +-----------------+------+------+
 SES uptime 0:00:04:20
```

Get address/Set address

Get ECC key

```
Available options:

 1 - Terminal mode
 2 - Get SERAM metrics
 3 - Get ECC key
 4 - Get Firewall configuration

Select an option (Enter to return): 3
ECC key (HEX):  26E6434B17CE4227585BE3068A05322196005A5349E2D1A7A9D9AE8185DDE76DC5C20DB614A64227AB218D514E76F248EEFD4B46C4AF87602C123A0BFF56E5AF
```

Get Firewall configuration

```
FC: 3 region: 2
FC: 3 region: 3
FC: 3 region: 4
FC: 3 region: 5
FC: 3 region: 6
FC: 3 region: 7
FC: 3 region: 8
FC: 3 region: 9
FC: 3 region: 10
FC: 3 region: 11
FC: 3 region: 12
FC: 3 region: 13
FC: 3 region: 14
FC: 3 region: 15
FC: 3 region: 16
FC: 3 region: 17
FC: 3 region: 18
FC: 3 region: 19
FC: 3 region: 20
FC: 3 region: 24
FC: 3 region: 25
FC: 3 region: 26
FC: 3 region: 27
FC: 3 region: 28
FC: 3 region: 29
FC: 3 region: 32
FC: 3 region: 33
FC: 3 region: 39
FC: 4 region: 0
FC: 4 region: 1
FC: 5 region: 0
FC: 5 region: 1
```

```
Available options:

 1 - Enable LOGGING
 2 - Disable LOGGING
 3 - Enable PRINTING
 4 - Disable PRINTING
```

Enable / Disable LOGGING

Enable / Disable PRINTING

Top level menu group

```
Available options:

 1 - Recovery
 2 - Recovery (No Reset)

Select an option (Enter to return):

Available options:

 1 - Device Control
 2 - Device Information
 3 - MRAM
 4 - Utilities
 5 - Setting capabilities
 6 - ROM

Select an option (Enter to exit):
```

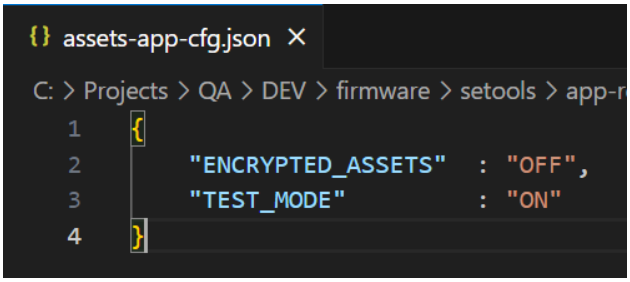
Recovery Session

```
Available options:

 1 - Recovery
 2 - Recovery (No Reset)

Select an option (Enter to return): 1
Bootloader stage: SEROM
Bring Up mode - Blank part detected!
Detected Part#: AE722F80F55D5LS
Detected Revision: B4
Device is not provisioned!
[INFO] System TOC Recovery with parameters:
- Device Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B4
- MRAM Base Address: 0x80580000
alif\SP-AE722F80F55D5LS-rev-b4-dev.bin[####################]100%: 270368/270368 bytes
[INFO] recovery time     110.68 seconds
alif\offset-58-rev-b4-dev.bin   [####################]100%: 16/16 bytes
[INFO] recovery time       0.00 seconds
[INFO] Target reset
```

ALIF
SEMICONDUCTOR

Target not in recovery mode

build\config\assets-app-cfg.json



-
  -
  -
-
  -
  -

$ app-assets-gen (-h for help)

```
C:\SETOOLS>app-assets-gen.exe
Generating APP assets with:
- Device Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- Configuration file: build/config/assets-app-cfg.json
- Output file: build/assets-app-cfg.bin

Creating Assets Package...
Checking Assets Package...
Package integrity Ok!
AssetID: APPASSET
Asset Version: 1

Provisioning Options:
ENCRYPTED_ASSETS        OFF
TEST_MODE           ON

Done!
```

$ app-assets-gen -c

```
C:\SETOOLS>app-assets-gen.exe -c
Generating APP assets with:
- Device Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- Output file: build/assets-app-cfg.bin

Checking Assets Package...
```

Example:

$ app-assets-gen -f build\config\assets-cfg.json
$ app-assets-gen -c –f build\assets-cfg.bin

$ app-provision (-h for help)

```
C:\SETOOLS>app-provision.exe
APP Provision with parameters:
Device Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
Assets file: build/assets-app-cfg.bin

[INFO] COM12 open Serial port success
[INFO] Running APP Provisioning code...
←[94m APP Provision ran in TEST MODE!
 ←[0m
[INFO] Done
```

build\assets-app-cfg.bin

```
C:\SETOOLS>app-assets-gen.exe
Generating APP assets with:
- Device Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
- Configuration file: build/config/assets-app-cfg.json
- Output file: build/assets-app-cfg.bin

Creating Assets Package...
Checking Assets Package...
Package integrity Ok!
AssetID: APPASSET
Asset Version: 1

Provisioning Options:
ENCRYPTED_ASSETS        OFF
TEST_MODE               OFF

Done!
```

```
C:\SETOOLS>app-provision.exe
APP Provision with parameters:
Device Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
Assets file: build/assets-app-cfg.bin

[INFO] COM12 open Serial port success
[INFO] Running APP Provisioning code...
←[94m APP Provision Return Code: 0x0
 ←[0m
[INFO] Done
```

```
C:\Windows\System32\cmd.exe - maintenance.exe
Select an option (Enter to return): 1
[TERMINAL] Ctrl-C to exit
|

SEROM v0.47.68 0x0000B200

[SES] Cold boot path
*** Host Firewall configured

[SES] MRAM error bypass is Enabled


SES B0 EVALUATION_BOARD v1.0.87 Dec  8 2023 23:59:45
[SES] Device ID = 0x0000B200
[SES] PLL code version 0.0.4
[SES] LCS=5
[SES] System partition address  0x80580000
[DEV] Wounding Data: 0x00C0FFFB
[SES] System      device configuration processed (0x00000000) BL_STATUS_OK
[SES] Application device configuration processed (0x00000001) BL_ERROR_APP_INVALID_TOC_ADDRESS
[SES] System      partition processed (0x00000000) BL_STATUS_OK
[SES] Application partition processed (0x00000001) BL_ERROR_APP_INVALID_TOC_ADDRESS
```

-
-

```
$ app-secure-debug  (-h for help)
```

```
C:\Windows\System32\cmd.exe

C:\Projects\QA\DEV\app-release>python3 app-secure-debug.py
Secure Debug with parameters:
Device Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
[INFO] COM12 open Serial port success
[INFO] Alif secure debug
Creating Signature...
Binary File:  ../build/alif_secure_debug.bin
2024-03-04 11:43:55,787 - Content Certificate Generation Utility started (Logging to ../build/logs/SBContent.log)
Content Certificate File:  build/alif_secure_debug.bin.crt
Signature File:  build/alif_secure_debug.bin.sign
Verify Certificate
Signature File:  build/alif_secure_debug.bin.sign


C:\Projects\QA\DEV\app-release>
```

$ app-secure-debug --rma

```
C:\Windows\System32\cmd.exe

C:\Projects\QA\DEV\app-release>python3 app-secure-debug.py --rma
Secure Debug with parameters:
Device Part# E7 (AE722F80F55D5LS) - 5.5 MRAM / 13.5 SRAM - Rev: B2
[INFO] COM12 open Serial port success
[INFO] Alif secure debug
Creating Signature...
Binary File:  ../build/alif_secure_debug.bin
2024-03-04 11:48:57,040 - Content Certificate Generation Utility started (Logging to ../build/logs/SBContent.log)
Content Certificate File:  build/alif_secure_debug.bin.crt
Signature File:  build/alif_secure_debug.bin.sign
Verify Certificate
Signature File:  build/alif_secure_debug.bin.sign


C:\Projects\QA\DEV\app-release>
```

-
-

```
$ python3 updateSystemPackage.py -m isp -x
Burning: System Package in MRAM
Device Part# AE722F80957D2CH - Rev: A0
- MRAM Base Address: 0xa0580000


alif\header.bin                 [####################]100%: 48/48 bytes
alif\SystemPackage.bin          [####################]100%: 281280/281152 bytes
RX<--  length=   4 command= COMMAND_NAK            chksum= 0x6 error= ISP_BAD_DEST_ADDRESS
```

```
Available options:

1 - maintenance mode
2 - device reset
3 - device enquiry
4 - get revision info
5 - get TOC info

Select an option: 4
[ERROR] Target did not respond
```

-
-

-
-
-
-

```
[TERMINAL] Ctrl-C to exit
\

SEROM v1.93.1 0x0000A001
[SEROM] BOOT_LOADER_find_and_load_seram(): error: 0x00000030; extended error code: 0x00000000
[SEROM] LCS = 0x0

[SEROM][ 0x7A606000 ] MRAM_CONTROLLER_BASE_ADDRESS = 0x00000000
[SEROM][ 0x7A606004 ] MRAM_CONTROLLER_FSM_STATE    = 0x00000000
[SEROM][ 0x7A606008 ] MRAM_CONTROLLER_ERROR_CAUSE  = 0x00000000
[SEROM][ 0x7A60600C ] MRAM_CONTROLLER_PENDING_0    = 0x00000000
[SEROM][ 0x7A606010 ] MRAM_CONTROLLER_PENDING_1    = 0x00000000


Dump trace buffer
0x037B0105 0x03873E0A 0x0000003F 0x35E5020D 0x35F30311 0xC91D0415 0x03990519 0x10CD311E 0x00000001 0x10D93122
0x00000000 0x11018526 0x001FFFF0 0x110F862A 0x00000000 0xCD210F2D 0x34790631 0x34AD0735 0x0C5F1039 0x0BE3343D
0x62991D42 0x00000030 0x62A33646 0x00000000 0xD99DFE09 0x4AD85CEB 0x978CBCD4 0x337A8FA3 0x66E0781B 0xFFB5BEEF
0xBF8DC6D8 0x0BEAEDB8 0x9DEAA2BC 0xFCDFC46E 0x73E7276E 0x1C2FE577 0xFA7E653B 0xEF7F7132 0x3F7FF876 0x2B7207A9
0xCDE88D3F 0x5E943CB7 0x7E3E229E 0xA705CE1D 0x7DE01AAF 0xEE1B3A15 0xEEF6139F 0x84CFDBAF 0xB6FD75E4 0x374538F7
0xAE33FE7C 0x2C3CAB33 0x76E678FB 0xE5F2099B 0xE2CB7ED7 0x977AA123 0x763BB1A5 0x448E982B 0x584D05B3 0x7E7BCCE3
0xDD1C94C7 0x8A5A9A9F 0xC8D09ABB 0x6D74FD3C 0x00111118 0xEEEEEEEE 0x4D4DAF67 0x97FD6316 0x9D5F776E 0xB150F922
0xD02611B5 0xBFE37D82 0xF9EEF977 0x014F9573

[SEROM] Mfg data
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

[SEROM] Serial No.
0x00000000 0x00000000

[SEROM] GPIO breadcrumb = 0x00003000
[SEROM] Entering recovery mode...
```

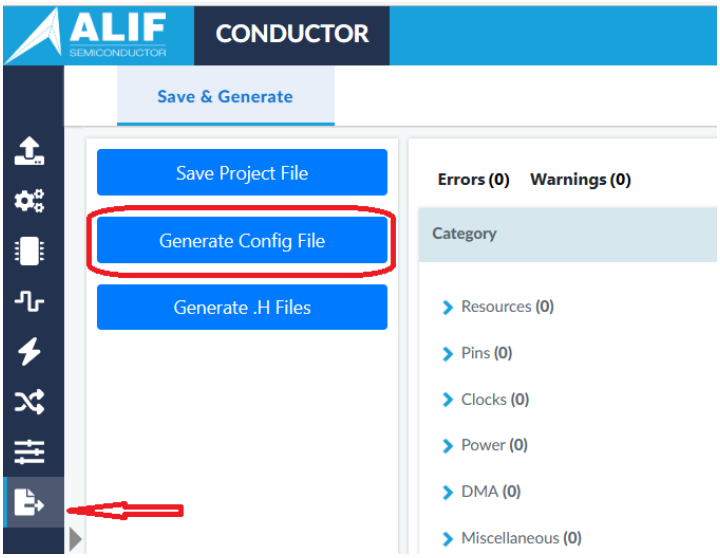
```
// Error codes
#define SEROM_STATUS_SUCCESS                          0x0

// Crypto errors
#define SEROM_BSV_INIT_FAIL                           0x1
#define SEROM_BSV_LCS_GET_AND_INIT_FAIL               0x2
#define SEROM_BSV_LCS_GET_FAIL                        0x2
#define SEROM_BSV_SEC_MODE_SET_FAIL                   0x3
#define SEROM_BSV_PRIV_MODE_SET_FAIL                  0x4
#define SEROM_BSV_CORE_CLK_GATING_ENABLE_FAIL         0x5
```

```
// MRAM errors
#define SEROM_MRAM_INITIALIZATION_FAILURE              0x6
#define SEROM_MRAM_INITIALIZATION_TIMEOUT              0x7
#define SEROM_MRAM_WRITE_FAILURE                       0x8


// ATOC errors
#define SEROM_ATOC_EXT_HDR_OFFSET_ZERO                 0x9
#define SEROM_ATOC_EXT_HDR_OFFSET_TOO_LARGE            0xA
#define SEROM_ATOC_OBJECT_OFFSET_ZERO                  0xB
#define SEROM_ATOC_OBJECT_OFFSET_MISALIGNED            0xC
#define SEROM_ATOC_OBJECT_OFFSET_TOO_LARGE             0xD
#define SEROM_ATOC_OBJECT_OFFSET_TOO_SMALL             0xE
#define SEROM_ATOC_EXT_HDR_OFFSET_MISALIGNED           0xF
#define SEROM_ATOC_HEADER_OFFSET_INVALID               0x10
#define SEROM_ATOC_HEADER_CRC32_ERROR                  0x11
#define SEROM_ATOC_HEADER_STRING_INVALID               0x12
#define SEROM_ATOC_NUM_TOC_ENTRIES_INVALID             0x13

// Certificate errors
#define SEROM_CONTENT_CERTIFICATE_NULL                 0x14
#define SEROM_CERTIFICATE_NULL                         0x15
#define SEROM_CERTIFICATE_CHAIN_INVALID                0x16
#define SEROM_INVALID_OEM_ROT                          0x17
#define SEROM_CERTIFICATE_ERROR_BASE                   0x18
#define SEROM_CERTIFICATE_1_ERROR                      0x19
#define SEROM_CERTIFICATE_2_ERROR                      0x1A
#define SEROM_CERTIFICATE_3_ERROR                      0x1B

// BOOT errors
#define SEROM_BOOT_CODE_LOAD_ADDR_INVALID              0x1C
#define SEROM_BOOT_VERIFY_IN_MEMORY_CASE_INVALID       0x1D
#define SEROM_BOOT_ZERO_IMAGE_LENGTH_INVALID           0x1E
#define SEROM_BOOT_ENCRYPTED.024 Tc[(definm)3         0x1e
```

ALIF SEMICONDUCTOR

-
-
-

-
-
-



\build\config

app-device-config-test.json

-
-
-
-
-
-

```
[INFO] Create area for: miscellaneous
[INFO] Process Miscellaneous
[INFO] [WARN] SE not supported:  ISP_MAINTENANCE_SUPPORT
[INFO] [WARN] SE not supported:  FW_RUNTIME_CFG
[INFO] [WARN] SE not supported:  PINMUX_RUNTIME_CFG
[INFO] [WARN] SE not supported:  CLOCK_RUNTIME_CFG
[INFO] [WARN] SE not supported:  BOARD_LED_COUNT
[INFO] [WARN] SE not supported:  BOARD_LEDRGB_COUNT
[INFO] [WARN] SE not supported:  BOARD_BUTTON_COUNT
[INFO] [WARN] SE not supported:  BOARD_CONFIG_JUMPER_COUNT
[INFO] [WARN] SE not supported:  BOARD_SWITCH_OUTPUT_COUNT
Calculating APP area...
```


-

C:\Windows\System32\cmd.exe - python3 maintenance.py

```
3 - Get CPU boot info
4 - Device enquiry
5 - Get revision info
6 - Get OTP data
7 - Get MRAM data
8 - Get log data
9 - Get SEROM trace data
10 - Get SERAM trace data
11 - Get power data
12 - Get clock data

Select an option (Enter to return): 4
SEROM Error =  0x24 (SEROM_BOOT_FAILED)  Extended Error =  0xf1000015 Maintenance Mode = <None>
```

-

2. Recovery (No Reset)

-

-
-
-
-
  -
-

Version	Date	Change Log