



# ENSEMBLE B2 / B3 / B4 BALLETTTO B1C / E1C

## SES (Secure Enclave Supervisor) Software

DEV V1.101.0

Release notes

## Table of Contents

### Contents

Table of Contents.....	2
Software Release Version .....	3
New Features in this Release.....	4
Updates / Fixes this Release .....	4
Removed / Deprecated in this Release.....	4
Release Output .....	5
Release Known Limitations and Issues .....	6
Features Not implemented.....	6
BUGS - Ensemble.....	7
SES Feature Default Build Options.....	8
PLL Versions REV_B0.....	10
Version 0.0.3 .....	10
SETOOLS Versions .....	11



## Software Release Version

This version of software is Tagged with version **SE\_FW\_1.101.0**

Component	DEV Version
SERAM (Secure Enclave Random Accesses Memory)	V1.101.0
SEROM (Secure Enclave Read Only Memory)	V1.1010
PLL_REV_B0	V0.0.4

Please see Version String in this release note.

Please see Release Known Limitations and Issues in this release note.

Please see Release Feature Specifics for details of all changes in this release.

## New Features in this Release

- SES Implemented proper initialization of the internal CMAC contexts, which allows the CMAC functions to execute correctly.
- Host MHU Secure firewall config
- SETOOLS gen-toc.py handling unsigned SERAM images.
- SETOOLS Full UPD packages are now in the app-release.

## Updates / Fixes this Release

- INTERNAL ARM Compiler updates for switch.
- SERVICES
  - o SERVICES Version: 0.50.1
  - o Contributed power examples updates.
  - o Documentation update on SERVICES\_boot\_process\_toc\_entry() and use of DEFERRED.
  - o Documentation update on SERVICES\_system\_get\_toc\_version() which is a deprecated function.
- BUG FIXES:
  - o [JIRA] (SE-2830) [SETOOLS] Firmware version is not getting updated in the TOC table
  - o [JIRA] (SE-2808) [SETOOLS] Few of the screenshots need to be added in the SETOOLS documentation
  - o [JIRA] (SE-2826) [SERVICES] app-device-config.json is not copied by 'make install'
  - o [JIRA] (SE-2818) [BOLT][aiPM] Chip/Application does not wake up after STOP mode
  - o [JIRA] (SE-2816) [BOLT][aiPM] Firewall Exception when PD5 is Off and wakes up without interrupt set from M55
  - o [JIRA] (SE-2811) [SETOOLS] gen-toc.py allocates the same SERAM bank when the same binary is specified
  - o [JIRA] (SE-2804) [SERVICES] Bounds Test shows random service response code with armclang
  - o [JIRA] (SE-2803) [SERAM] E1C UPD unsigned image causes recovery mode
  - o [JIRA] (SE-2638) [SETOOLS][REV\_B2] Trace marker for READ SOC\_ID is not consistent
  - o [JIRA] (SE-2798) [SERAM] Cold wake up bit left ON
  - o [JIRA] (SE-2848) [REV-B4][SETOOLS] Override SOC\_ID trace is seen in both SERAM and SEROM trace data
  - o [JIRA] (SE-2711) [SERAM] Storage address is not shown in SEUART for Deferred images
  - o [JIRA] (SE-2611) [SERAM] Trace entries must be voided before rolling over buffer
  - o [JIRA] (SE-2565) [SETOOLS][REV\_B3] OTP Mfr Data decode

## Removed / Deprecated in this Release.

- <>



## Release Output

SE UART output:

NOTE: We **strongly** recommend you have the SE-UART connected.

```
COM7 - Tera Term VT
File Edit Setup Control Window Help

[SEROM v1.96.0 0x0000B400

[SES B4 v1.101.0 Sep 27 2024 23:28:22
[SES] No ATOC
[SES] System partition address 0x80580000
[SES] STOC DEVICE ok
[SES] No LF XIAL

[SES] SERAM bank 0x0 is valid and booted
[SES] STOC ok
[SES] MS5-HE booted from address 0x58000000
[SES] LCS=1
[SES] PC: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 U   | 15.74    |
| * SERAM0 | CM0+  |           | 0x000000C0 |           |           | 83408 | 1.101.0 |       | 0.00     |
| SERAM1  | CM0+  |           | 0x00020AC0 |           |           | 83408 | 1.101.0 |       | 0.00     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
Legend: <u><C>ompressed,<L>oaded,<U>erified,<s>kipped verification,<B>ooted,<E>ncrypted,<D>eferred

[SES] SE frequency is 99.82 MHz
[SES] os Kernel U10.4.2 <Tickless>
[SES] Main Task - looping forever...
-
```

The version of SES is always printed (see above). See Developer Mode / Version String for alternative methods of finding the SES version.

[SEROM] Device ID	Shows the device ID as returned from the soc_id register.
[SES] LCS	Life Cycle State (0 = CM, 5 = DM, 7 = Secure)
[SES] System partition	Where does the STOC start in MRAM.
[SES] STOC Part# match	Error code checking Device part# with the image build.
[SES] System partition	Error code from processing STOC or OK
[SES] Application partition	Error code from processing ATOC or OK

## Release Known Limitations and Issues

Features Not implemented.

[JIRA] (SE-1827) [SERAM] Security Settings	DCT “Misc” Page for SE
[JIRA] (SE-1082) [SESW] OTA Strategy	OTA update strategy. Stage#3 (Partial) TBD
A32 bare metal SERVICES	This is not supported in CMSIS
LINUX SERVICES	Linux based SERVICE library

## BUGS - Ensemble

SE-2868	[BOLT-B4][aiPM] Hard fault with BASIC4 demo application for STOP mode	aiPM
SE-2821	Hard fault on SERAM resume from standby when MRAM header switch is off	aiPM
SE-2665	SRAM(s) not powered up when waking up from stop mode (v1.96.0)	aiPM
SE-2663	HP core never wakes up from stop if wake up interrupt happens during the stop sequence	aiPM
SE-2599	[aiPM] If both M55 cores set ip_clock_gating to zero, then (NPU_HP_MASK   NPU_HE_MASK   LP_PERIPH_MASK) can't be turned on	aiPM
SE-2347	[aiPM] Incomplete logs with STOP mode test application ( services_aipm_stop_modes)	aiPM
SE-2346	[aiPM] Incomplete logs with READY mode application	aiPM
SE-2333	[aiPM] HP is not going to local OFF with GO mode application(services_aipm_go_modes) mode-5	aiPM
SE-2332	[aiPM] Standby mode application(services_aipm_standby_modes) isn't functioning as intended.	aiPM
SE-2813	[SERAM] Trace decoder inconsistent	SES
SE-2803	[SERAM] E1C UPD unsigned image causes recovery mode	SES
SE-2611	[SERAM] Trace entries must be voided before rolling over buffer	SES
SE-2277	[SERAM] STOP mode race condition handling	SES
SE-1936	[SETOOLS] Maintenance / Get MRAM data bounds check failure	SETOOLS
SE-2867	[BOLT-B4] [Services] UPD image is not getting updated with demo application	SERVICES
SE-2852	[REV-B3][Services] Target goes into unresponsive when RESET_CPU service_api is ran continuously from TCM	SERVICES
SE-2845	[services] Using SERVICES_system_get_toc_data API is not giving all the flags in the table	SERVICES
SE-2844	[Services] Improper functionality of 2 System Management services when given incorrect parameters	SERVICES
SE-2833	[BOLT] [Services] Deferred image boots up before the SERVICES_boot_process_toc_entry service request	SERVICES
SE-2815	[SERAM][SERVICES] AES decryption test produces incorrect data	SERVICES
SE-2549	ETR trace breaks when calling SERVICES_set_run_cfg	SERVICES
SE-1854	Invalid examples for SERVICES_pinmux and _padcontrol documentation	SERVICES
SE-1441	[SERVICES] A32 service requests NACKed	SERVICES
SE-1328	[SERVICES] A32 link register address incorrect	SERVICES

## SES Feature Default Build Options

Flag	State	Notes
WATCHDOG_SUPPORT	DISABLED	
OS_SUPPORT	ENABLED	
ISP_SUPPORT	ENABLED	
FLICKER_SUPPORT	ENABLED	
PLL_SUPPORT	ENABLED	
MRAM_ERROR_BYPASS	ENABLED	REV_B0 Only MRAM controller bypass
CPU_SPEED_CALCULATION_SUPPORT	ENABLED	
SERAM_MAINTENANCE_MODE_SUPPORT	ENABLED	
M55_TCM_FULL_RANGE	ENABLED	
SERAM_UART_RECOVERY	ENABLED	
TOC_CRC32_CHECK	ENABLED	
ENABLE_MODEM_JTAG	ENABLED	
PRINT_BOOT_MESSAGES	ENABLED	
CC_RT_SUPPORT	ENABLED	
CC_RT_ENABLE_LCS_OVERRIDE	ENABLED	
ENABLE_SIMBOLT_PRINT	DISABLED	
DISABLE_UART_BEFORE_PLL_INIT	DISABLED	
VERSION_STRING_WRITE_SUPPORT	DISABLED	
LOW_POWER_SUPPORT	DISABLED	
DEVICE_KEYPAIR_GENERATION	DISABLED	
BANK_MAINTENANCE_SUPPORT	DISABLED	
EFUSE_POWER_SUPPORT	DISABLED	
MBEDTLS_STATIC_ALLOCATOR	DISABLED	
HOUSE_KEEPING_TASK	DISABLED	
TRACE_BUFFER_SUPPORT	DISABLED	
CRYPTO_RT_SECURE_DEBUG	ENABLED	
CRYPTO_RT_READ_ECC_PUBLIC_KEY	ENABLED	
MAINTENANCE_FLAG_IN_MRAM	ENABLED	
DMPU_CODE	DISABLED	
ENABLE_BREADCRUMBS	DISABLED	SEROM
TRACE_SUPPORT	DISABLED	SEROM
TRACE_TIME_STAMP_SUPPORT	DISABLED	SEROM
ENABLE_SERAM_OEM_ROT	DISABLED	SEROM
BANK_SELECTION_SUPPORT	ENABLED	SEROM
FAST_BOOT_IN_SECURE_LCS	ENABLED	SEROM
ENABLE_CM55_HE_VTOR_CHECK	ENABLED	SEROM
ENABLE_MODEM_FAST_BOOT	DISABLED	SEROM
LOW_POWER_TESTING	DISABLED	SEROM



SHOW_WAKUP_COUNT	DISABLED	SEROM
CRYPTO_SERVICES_SUPPORT	ENABLED	
CRYPTO_SERVICES_GET_LCS_SUPPORT	ENABLED	
CRYPTO_SERVICES_GET_RND_SUPPORT	ENABLED	
CRYPTO_SERVICES_TRNG_POLL_SUPPORT	ENABLED	
CRYPTO_SERVICES_AES_SUPPORT	ENABLED	
CRYPTO_SERVICES_SHA_SUPPORT	ENABLED	
CRYPTO_SERVICES_CCM_SUPPORT	ENABLED	
CRYPTO_SERVICES_GCM_SUPPORT	ENABLED	
CRYPTO_SERVICES_CHACHA20_SUPPORT	ENABLED	
CRYPTO_SERVICES_CHACHAPOLY_SUPPORT	ENABLED	
CRYPTO_SERVICES_POLY1305_SUPPORT	ENABLED	
CRYPTO_SERVICES_CMAC_SUPPORT	ENABLED	

## PLL Versions REV\_B0

Version Number	JIRA	Description
0.0.3		REV_B0 bring up
0.0.2		PLL refactor
0.0.1		First incarnation

The version of the PLL is printed out during the boot up of SERAM.

The initial PLL for REV\_B0 was based on the one used by DV.

### Version 0.0.3

- Extra delay timings added.
- The short delay times did not give the PLL enough window to calibrate itself correctly. It was settling to a bias current code for the Oscillator which was too high.
  - When the PLL loop closes, it tries to force the frequency to  $2.4\text{GHz} = (38.4\text{M} / 2) \times 125$  by removing some of the current through NMOS device driven by VCO Vcontrol. Unfortunately, VCO Vcontrol can't go higher than 0.7V as measured through AMUX\_P resulting in PLL CLK been much higher than 2.4GHz.
  - We saw it at 2.9GHz which corresponds to 480MHz with Rev 0.0 SERAM image.

## SETOOLS Versions

Tool name	Version	ICV	APP	Notes
gen-toc.py	0.25.000	●		
gen-rot.py	0.06.000	●		
gen-otp.py	0.08.000	●		
app-gen-toc.py	0.28.002		●	
app-gen-rot.py	0.02.000		●	
app-provision.py	0.06.000		●	
app-write-mram.py	0.20.003		●	
UpdateAlifpackage.py	0.12.000		●	Deprecated in Release V0.29.00
updateSystemPackage.py	0.21.001		●	
lcv-provision.py	0.05.000	●		
write_image.py	0.18.004	●		
cert-check.py		●		
firewall.py		●		
load_image.py	0.01.000	●		
alif-image-check.py	0.11.000	●	●	
maintenance.py	0.06.000	●	●	
tools-config.py	0.01.000	●	●	
secure_debug.py	0.1.000			
recovery-seram.py	0.02.000	●	●	Deprecated in Release V0.41.00
icv-recovery.py	0.3.000	●		
recovery.py	0.3.000	●	●	REV_A1, B0 only
sign_image.py	0.1.000	●	●	ICV Release only

