By default Ram dump is disabled on a secure boot device for security reason. To get Ramdump on a secure boot enabled device:

NOTE :
These approaches should be used for debugging purpose only.
All security holes by customized ram dump approach(including TZ log) in secure boot enabled device MUST be customer's own responsibility and own risk because Qualcomm solution doesn't allow valid ram dump to avoid security hole after enabling secure boot.(e.g. reverse engineering.).

These changes should not be mainlined in production image.

1. Modify tzbsp_allow_memory_dump() as shown below.
trustzone_images\core\securemsm\trustzone\qsee\kernel\src\tzbsp_dload_mode.c

```
boolean tzbsp_allow_memory_dump()
{
+ if(tzbsp_is_dload_mode_set())
+ {
+ return TRUE;
+ }
+
+#if 0
#if defined FEATURE_DLOAD_MEM_DEBUG
<snip>
#endif
+#endif

/* By default memory dumping is denied. */
return FALSE;

}
```

2. Modify tzbsp_security_allows_mem_dump() to return E_SUCCESS.
trustzone_images\core\securemsm\trustzone\qsee\kernel\src\tzbsp_dload_mode.c

```
int tzbsp_security_allows_mem_dump(uint32 *rsp, uint32 rsplen)
{
<snip>
/* Populate the response and return success */
- *rsp = (uint32)(tzbsp_secboot_hw_is_auth_enabled(1) == 0 || tzbsp_is_debug_enabled() ||
tzbsp_is_retail_crash_dump_enable());
+ *rsp = (uint32)TRUE;

return E_SUCCESS;
}
```

3.Modify tzbsp_allow_unlock_xpu() to return TRUE.
MSM8916 - trustzone_images\core\securemsm\trustzone\qsee\arch\msm8916\src\tzbsp_sec_core.c
MSM8939 - trustzone_images\core\securemsm\trustzone\qsee\arch\msm8936\src\tzbsp_sec_core.c

```
boolean tzbsp_allow_unlock_xpu(void)
{
<snip>
/* By default memory dumping is denied. */
retval = (debug_flag ||
(!tzbsp_secboot_hw_is_auth_enabled(1) && !tzbsp_spiden_disable));
- return retval;
+ return TRUE;
}
```

4. When you need modem ramdump, you also need a following change in addition to the above.

```
modem_proc\core\securemsm\mba\src\oem\oem_mba_ac.c
uint8 mba_oem_seccrtl_allow_unlock_xpu(void)
{
- return FALSE;
+ return TRUE;
}
```

5. If you want to preserve RPM information in ramdump, you also need to be updated like as below.

```
MSM8916 - boot_images\core\boot\secboot3\hw\msm8916\sbl1\sbl1_config.c
MSM8939 - boot_images\core\boot\secboot3\hw\msm8936\sbl1\sbl1_config.c
/* Conditionally cancel RPM loading in SBL1 */
static boot_boolean rpm_load_cancel(bl_shared_data_type *bl_shared_data)
{
boot_boolean is_auth_enabled = FALSE;

bl_error_type status = boot_is_auth_enabled(&is_auth_enabled);
BL_VERIFY((status == BL_ERR_NONE), BL_ERR_IMG_SECURITY_FAIL);

/* Do not load RPM if we are in DLOAD mode and auth is disabled.
* This is to preserve RPM code ram for the memory debug tools */
- return (boot_boolean)(boot_dload_is_dload_mode_set() == TRUE &&
- is_auth_enabled == FALSE);
+ return (boot_boolean)(boot_dload_is_dload_mode_set() == TRUE)
}
```

6. To eanble TZ logging.

```
MSM8916 - trustzone_images\core\securemsm\trustzone\qsee\oem\msm8916\src\tzbsp_oem_log.c
MSM8939 - trustzone_images\core\securemsm\trustzone\qsee\oem\msm8936\src\tzbsp_oem_log.c
boolean tzbsp_oem_allow_logging(void)
{
+ return TRUE;
+#if 0
#ifdef VIRTIO_8962
#warning VIRTIO_8962: forcing logging in tzbsp_oem_allow_logging
return TRUE;
#endif
#ifndef TZBSP_RUMI
/* By default, logging is disabled if secure boot is enabled. */
if(tzbsp_secboot_hw_is_auth_enabled(1))
{
return FALSE;
}
else
{
#endif
return TRUE;
#ifndef TZBSP_RUMI
}
#endif
+#endif
}
```

7. Enable backup tz mem region (important for tz debug) but mandatory condition for this is CR#669584.(e.g . BOOT.BF.3.0-00248-M8936AAAAANAZB-1 has this CR.)

```
boot_images\core\boot\secboot3\src\boot_extern_seccfg_interface.c
boot_boolean boot_qsee_is_memory_dump_allowed(secboot_verified_info_type * secboot_info)
{
- return qsee_is_memory_dump_allowed(secboot_info);
+ return TRUE;
}
```