

# USER GUIDE AMD EPYC 9004, 7003, 7002, 7001



# Using SEV with AMD EPYC<sup>™</sup> Processors

Publication Revision Issue Date 58207 1.0 Mar, 2023

#### © 2023 Advanced Micro Devices, Inc. All rights reserved.

The information contained herein is for informational purposes only and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD's products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale.

#### Trademarks

AMD, the AMD Arrow logo, AMD EPYC, and combinations thereof are trademarks of Advanced Micro Devices, Inc. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

\* Links to third party sites are provided for convenience and unless explicitly stated, AMD is not responsible for the contents of such linked sites and no endorsement is implied.

Date	Version	Changes
Mar, 2023	1.0	Initial release

### Audience

This tuning guide is intended for a technical audience such as production deployment, virtualization developers, firmware engineers, and performance engineering teams with:

- A background in configuring servers.
- Access to the system BIOS.

### Author

Brent Hollingsworth, Diego Gonzalez Villalobos, Anthony Hernandez



# **Table of Contents**

Chapter 1	1	Security Features by Processor Generation	-1
1.1	1	4th Gen (9xx4)	1
1.	2	3rd Gen (7xx3)	1
1.3	3	2nd Gen (7xx2)	2
1.4	4	1st Gen (7xx1)	2
Chapter 2	2	Enabling/Disabling SMEE	-3
2.	1	Enabling SMEE in BIOS	3
		2.1.1 AMD EPYC 9004 Series Processors	3
		2.1.2 AMD EPYC 7003 Series Processors	6
		2.1.3 AMD EPYC 7002 and 7001 Series Processors	8
2.	2	Enabling SMEE via SMR	8
2.	3	Disabling SMEE in BIOS	9
		2.3.1 AMD EPYC 9004 Series Processors	9
		2.3.2 AMD EPYC 7003 Series Processors	9
		2.3.3 AMD EPYC 7002 and 7001 Series Processors	9
2.	4	Disabling SMEE via MSR	.10
2.	5	Enabling TSME on All Processors:	11
		2.5.1 Enabling TSME on All Processors	. 11
		2.5.2 Disabling TSME on All Processors	14
Chapter 3	3	Configuring SEV	15
3	1	AMD EDVE 9004 Series Processors	15
ן. ב	י ז	AMD EPVC 7003 and 7002 Series Processors	16
3	3	AMD EPYC 7001 Series Processors	17
5.			,
Chapter 4	4	Enabling/Disabling SNP	19
4.	1	Enabling SNP	. 19
4.	2	Disabling SNP	. 21
Chapter !	5	OS Requirements	23
5	1	SEV	23
5.	2	SEV-ES	23
5.	3	SEV-SNP	24

# AMD Using SEV with AMD EPYC<sup>™</sup> Processors

Chapter 6	OS Enablement	25
6.1	Checking SEV Enablement	25
6.2	Enabling SEV	25
	6.2.1 Additional Resources	
6.3	Enabling SEV-SNP	26
Chapter 7	Updating SEV Firmware	27
7.1	DownloadFirmware	27
7.2	DownloadFirmwareEX	29
Chapter 8	Launching an Encrypted VM	31
8.1	Launching a VM with SEV Encryption	
	8.1.1 Launching with QEMU	
	8.1.2 Launching with Libvirt	32
8.2	Launching a VM with SEV-ES Encryption	32
8.3	Launching a VM with SEV-SNP Encryption	33
Chapter 9	Confidential Containers	35
Chapter 10	Frequently Asked Questions	37
Chapter 11	Performance Data	41

# 

Chapter

# Security Features by Processor Generation

AMD EPYC processors have the following security features by generation:

# 1.1 4th Gen (9xx4)

- Secure Encrypted Virtualization (SEV)
- Secure Encrypted Virtualization Encrypted State (SEV-ES)
- Secure Nested Paging (SEV-SNP)
- 1006 ASID keys
- Transparent Secure Memory Encryption (TSME)

# 1.2 3rd Gen (7xx3)

- Secure Encrypted Virtualization (SEV)
- Secure Encrypted Virtualization-Encrypted State (SEV-ES)
- Secure Nested Paging (SEV-SNP)
- Either:
  - 509 ASID keys (in systems equipped with up to 8TB DRAM)
  - 253 ASID keys (in systems equipped with up to 16TB DRAM)
- TSME

# 1.3 2nd Gen (7xx2)

- Secure Encrypted Virtualization (SEV)
- Secure Encrypted Virtualization-Encrypted State (SEV-ES)
- Either:
  - 509 ASID keys (in systems equipped with up to 8TB DRAM)
  - 253 ASID keys (in systems equipped with up to 16TB DRAM)
- TSME

# 1.4 1st Gen (7xx1)

- Secure Encrypted Virtualization (SEV)
- Secure Encrypted Virtualization-Encrypted State (SEV-ES)
- 15 ASID keys
- TSME

Chapter

# **Enabling/Disabling SMEE**

This chapter describes how to enable the AMD Secure Memory Encryption (SMEE) feature. SMEE must be enabled in order to use all SEV features. All of the instructions shown in this chapter are based on AMD Custom Reference Boards (CRBs). The exact steps and images may vary by OEM and BIOS version..

# 2.1 Enabling SMEE in BIOS

This section describes to enable SMEE on AMD EPYC processors.

### 2.1.1 AMD EPYC 9004 Series Processors

SMEE is disabled by default on systems powered by AMD EPYC 9004 Series Processors because of incompatibility with certain Linux kernels. To enable SMEE:

1. Access your system BIOS.

Main Advanced Chips	Aptio Setup - AMI et Security Boot Save &	Exit Firmware Update
BIOS Vendor Core Version Compliancy Project Version Build Date and Time Access Level	American Megatrends 5.25 UEFI 2.8; PI 1.7 RTI1001_L3 x64 10/06/2022 16:39:34 Administrator	<ul> <li>Choose the system default language</li> </ul>
Is this BVM BIDS BVM BIDS version BVM Request ID BVM Requester BVM Request Time	NO	++: Select Screen f4: Select Item Enter: Select +(-: Change Dot
Total Memory	Total Memory: 1572864 MB (DDR5)	F1: General Help F2: Previous Values F3: Optimized Defaults
System Language	(English)	▼ F4: Save & Exit ESC: Exit
Versi	on 2.22.1283 Copyright (C)	2022 AMI AB

Figure 2-1: System BIOS (AMD EPYC 9004 Series Processors)

2. Select the **Advanced** tab.

Aptio Setup – AMI Main Advanced Chipset Security Boot Save & Exit Firmware Update I		
SMM Lock Status [Enabled] HITT/WITT Selection [Both Disabled] Trusted Computing PSP Firmware Versions ACPI Settings CRB Board AMD CBS Debug UART Selection Serial Port Console Redirection CPU Configuration Debug Port Table Configuration PCI Subsystem Settings USB Configuration Network Stack Configuration CSM Configuration NVMe Configuration SATA Configuration	Setting to Enable/Disable SMM Lock #*: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1283 Copyright (C) 2	AB	

Figure 2-2: BIOS Advanced tab (AMD EPYC 9004 Series Processors)

3. Select AMD CBS.

Aptio Setup -	AMI
AMD CBS AMD CBS Revision 0x0 Number > DPU Common Options > DF Common Options > UMC Common Options > NBIO Common Options > FCH Common Options > NTB Common Options > Soc Miscellaneous Control > Workload Tuning > CXL Common Options	CPU Common Options ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1283 Copyri	ght (C) 2022 AMI AB

Figure 2-3: AMD CBS tab (AMD EPYC 9004 Series Processors)

Chapter 2: Enabling/Disabling SMEE

#### 4. Select **CPU Common Options**.

Advanced	Aptio Setup –	AMI
CPU Common Options		Performance
Performance		
REP-MOV/STOS Streaming Prefetcher settings Core Watchdog	[Enabled]	
RedirectForReturnDis	[Auto]	
Platform First Error Handling	[Auto]	
Core Performance Boost	[Auto]	++: Select Screen
Global C-state Control	[Auto]	11: Select Item
Power Supply Idle	[Auto]	Enter: Select
Control		+/-: Change Opt.
SEV-ES ASID Space	1	F1: General Help
Limit		F2: Previous Values
SEV Control	[Enable]	F3: Optimized Defaults
		▼ F4: Save & Exit
		ESC: Exit

Figure 2-4: CPU Common Options tab (AMD EPYC 9004 Series Processors)

5. Scroll down this tab, then select **SMEE**, and then set it to **Enable**.

Aptio Setup - AMI Advanced		
SEV-ES ASID Space Limit SEV Control Streaming Stores Control Local APIC Mode ACPI _CST C1 Declaration ACPI CST C2 Latency MCA error thresh enable MCA FruText SMU and PSP Debug Mode PPIN Opt-in SNP Memory (RMP Table) Coverage SMEE Action on BIST Failure	1 [Enable] [Auto] [Auto] [Auto] [Auto] [Auto] [Auto] [Auto] [Auto] [Auto] [Enable] [Auto]	<ul> <li>Control secure memory encryption enable Enabling both SMEE and SME-MK is not supported. Results in #GP</li> <li>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</li> </ul>
Versio	n 2.22.1283 Copyright	ESC: Exit (C) 2022 AMI

Figure 2-5: SMEE enabled (AMD EPYC 9004 Series Processors)

### 2.1.2 AMD EPYC 7003 Series Processors

SMEE is disabled by default on systems powered by AMD EPYC 7003 Series Processors because of incompatibility with certain Linux kernels. To enable SMEE:

1. Access your system BIOS.

Main Advanced Chips	Aptio Setup – AMI et Security Boot Save &	Exit Event Logs
BIOS Information		Choose the system
BIOS Vendor	American Megatrends	default language
Core Version	5.20	
Compliancy Project Version	UEFI 2.8; FI 1.7	
Build Date and Time	01/30/2022 00:51:46	
Access Level	Administrator	
Is this B∨M BIOS	No	
BVM BIOS version		
BVM Request ID		the Select Screen
BVM Request Time		Fotor: Select
byn negaest rine		+/-: Change Opt.
Memory Information		F1: General Help
Total Memory	Total Memory: 16384 MB	F2: Previous Values
	(DDR4)	F3: Optimized Defaults
		F9: Save & EXIT

Figure 2-6: System BIOS (AMD EPYC 7003 Series Processors)

#### 2. Select the **Advanced** tab.

Aptio Setup – AMI Main Advanced Chipset Security Boot Save & Ex	kit Event Logs
SMM Lock Status [Enabled] MITT/WITT Selection [Both Disabled] Trusted Computing PSP Firmware Versions ACPI Settings CRB Board AMD CBS Serial Port Console Redirection CPU Configuration	Setting to Enable/Disable SMM Lock
<ul> <li>PCI Subsystem Settings</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> <li>SATA Configuration</li> </ul>	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values
► AMD Mem Configuration Status	F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.21.1278 Copyright (C) 20	)22 AMI

Figure 2-7: BIOS Advanced tab (AMD EPYC 7003 Series Processors)

#### 3. Select AMD CBS.

Advanced	tio Setup — AMI	
AMD CBS > CPU Common Options > DF Common Options > UMC Common Options > NBID Common Options > FCH Common Options > Soc Miscellaneous Control > Workload Tuning	CPU Common Options ++: Select Screen +1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.21.1278 Copyright (C) 2022 AMI		

Figure 2-8: AMD CBS tab (AMD EPYC 7003 Series Processors)

#### 4. Select CPU Common Options.

Aptio Setup – AMI Advanced			
CPU Common Options		Performance	
<ul> <li>Performance</li> <li>Prefetcher settings</li> <li>Core Watchdog</li> </ul>			
RedirectForReturnDis Platform First Error Handling	[Auto] [Auto]		
Core Performance Boost Global C-state Control Power Supply Idle Control	[Auto] [Auto] [Auto]	<pre>++: Select Screen  ↑↓: Select Item Enter: Select</pre>	
SEV ASID Count SEV—ES ASID Space Limit Control	(Auto) (Auto)	+/−: Change Opt. F1: General Help F2: Previous Values	
Streaming Stores Control	(Auto)	F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit	
Version 2.21.1278 Copyright (C) 2022 AMI			

Figure 2-9: CPU Common Options tab (AMD EPYC 7003 Series Processors)

5. Scroll down this tab, then select **SMEE**, and then set it to **Enable**.

Streaming Stores	[Auto]	Control secure memory
Local ARTS Mode	[Auto]	encryption enable
ACDI ACI CI	[Huto]	
HEPI _CSI CI	[Huto]	
MCA appoint thrach	[outo]	
enable		
SMU and PSP Debug Mode	faut Disable	
PPIN Ont-in	faut Enable	
SNP Memory (RMP	faut Auto	
Table) Coverage		++: Select Screen
SMEE	[Auto]	↑↓: Select Item
Action on BIST Failure	[Auto]	Enter: Select
Fast Short REP MOVSB	(Auto)	+/-: Change Opt.
(FSRM)		F1: General Help
Enhanced REP	[Auto]	F2: Previous Values
MOVSB/STOSB (ERMSB)		F3: Optimized Defaults
REP-MOV/STOS Streaming	[Disabled]	▼ F4: Save & Exit
		ESC: Exit

Figure 2-10: SMEE enabled (AMD EPYC 7003 Series Processors)

### 2.1.3 AMD EPYC 7002 and 7001 Series Processors

SMEE is **Enabled** by default on system powered by AMD EPYC 7002 or 7001 Series Processors.

# 2.2 Enabling SMEE via SMR

To enable SMEE via the processor MSR:

- x86 can set the SMEE bit (bit 23) in the SYS CFG MSR before OS boot.
- MSRC001\_0010 [System Configuration] (Core::X86::Msr::SYS\_CFG)
- EDK2-based BIOS (non-CBS users) should specifically toggle this bit to enable/disable SEV if a reciprocal PCD method is not available for that processor family.

Note: This bit must be set on every CPU in the system.

Note: The bit is Write-1-Only, which (cannot be cleared once set, and which is set to 0 on system reset.

Note: AMD EPYC 7001 and 7002 Series Processors have SMEE enabled automatically. If SMEE is disabled in BIOS, then you can use MSR to reenable SMEE in the system.

Chapter 2: Enabling/Disabling SMEE

#### 2.3 **Disabling SMEE in BIOS**

This section describes disabling SMEE on AMD EPYC processors.

#### AMD EPYC 9004 Series Processors 2.3.1

To disable SMEE on a system with an AMD EPYC 9004 Series Processor:

- 1. Access your system BIOS.
- 2. Select the **Advanced** tab.
- 3. Select AMD CBS.
- 4. Select CPU Common Options.
- 5. Scroll down this tab, then select **SMEE**, and then set it to either **Auto** or **Disabled**.

#### 2.3.2 AMD EPYC 7003 Series Processors

To disable SMEE on a system with an AMD EPYC 7003 Series Processor:

- 1. Access your system BIOS.
- 2. Select the **Advanced** tab.
- 3. Select AMD CBS.
- 4. Select CPU Common Options.
- 5. Scroll down this tab, then select **SMEE**, and then set it to either **Auto** or **Disabled**.

#### AMD EPYC 7002 and 7001 Series Processors 2.3.3

You cannot disable SMEE on a system with an AMD EPYC 7002 or 7001 Series Processor.

# 2.4 Disabling SMEE via MSR

SMEE cannot be disabled in the MSR; the bit is Write-1-Only. You must either reset the system or disable SMEE in BIOS.

Note: Disabling SEV will allow the use of more than 16TB of system physical address space (DRAM + PCIe + MMIO, etc.) because x bits of physical address space will not be used for ASIDs/c-bit.

- AMD EPYC 9004 Series Processors: 52-bit addressing with no c-bit, SMEE/SEV off.
  - 46-bit address with SEV (1006 keys).
- AMD EPYC 7003 Series Processors: 48-bit addressing with no c-bit, SMEE/SEV off.
  - 43-bit address with SEV in 509-key mode, 44-bit in 253 key mode.
- AMD EPYC 7002 Series Processors: 48-bit addressing with no c-bit, SMEE/SEV off.
  - 43-bit address with SEV in 509-key mode, 44-bit in 253 key mode.
- AMD EPYC 7001 Series Processors: 48-bit addressing with c-bit, SMEE/SEV off.
  - 43-bit address with SME/SEV (16 keys).

٠

# 2.5 Enabling TSME on All Processors:

Transparent Secure Memory Encryption (TSME, also known as Secure Memory Encryptio) uses a single key to encrypt system memory. The AMD Secure Processor generates this key at boot. TSME requires enablement in the system BIOS and offers transparent memory encryption that can run with any operating system. TSME is separate from SEV, and you need not run SEV in order to benefit from TSME. TSME is disabled by default.

### 2.5.1 Enabling TSME on All Processors

To enable TSME on an AMD CRB:

- 1. Access the system BIOS.
- 2. Select Advanced.

Main Advanced Chip	Aptio Setup - AMI set Security Boot Save &	Exit Firmware Update
BIOS Information BIOS Vendor Core Version Compliancy Project Version Build Date and Time Access Level	American Megatrends 5.25 UEFI 2.8; PI 1.7 RTI1001_L3 x64 10/06/2022 16:39:34 Administrator	▲ Choose the system default language
Is this BVM BIOS BVM BIOS version BVM Request ID BVM Requester BVM Request Time Memory Information	NO	++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help
Total Memory	Total Memory: 1572864 MB (DDR5)	F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Vers	ion 2.22.1283 Copyright (C)	2022 AMI AB

#### 3. Select AMD CBS.

Main Advanced Chipset	Aptio Setup - Security Boot	AMI Save & E	xit	Firmware Update
SHM Lock Status MITT/WITT Selection Trusted Computing PSP Firmware Versions ACPI Settings CRB Board AHD CBS Debug UART Selection Serial Port Console Redi CPU Configuration Debug Port Table Configu PCI Subsystem Settings USB Configuration Network Stack Configurat CSM Configuration NVMe Configuration SATA Configuration	(Enabled) (Both Disabled)		AMD ++: T1: Ent: +/- F1: F2: F3: F4: ESC	CBS Setup Page Select Screen Select Item er: Select : Change Opt. General Help Previous Values Optimized Defaults Save & Exit : Exit
Version	2.22.1283 Copyri	ght (C) 2	022	AMI AB

#### 4. Select UMC Common Options.

Apti Advanced	o Setup – AMI	
AMD CBS AMD CBS Revision 0x0		UMC Common Options
<ul> <li>CPU Common Options</li> <li>DF Common Options</li> <li>UMC Common Options</li> <li>NBIO Common Options</li> <li>FCH Common Options</li> <li>NTB Common Options</li> <li>Soc Miscellaneous Control</li> <li>Workload Tuning</li> <li>CXL Common Options</li> </ul>	⊳	<pre>++: Select Screen f1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2.22.12	83 Copyright (C)	2022 AMI AB

Chapter 2: Enabling/Disabling SMEE

#### 5. Select DDR Security.

Aptio Setup - A Advanced	ні
UHC Common Options > DOR Addressing Options > DDR Controller Configuration > DOR MBIST Options > DOR RAS > DOR Bus Configuration > DOR Training Options > DOR Security > DOR PHIC Configuration > DDR PHIC Configuration > DDR Miscellaneous	DDR Security ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1283 Copyrigh	t (C) 2022 AMI AB

#### 6. Set **TSME** to **Enabled**.



### 2.5.2 Disabling TSME on All Processors

To disable TSME on an AMD CRB:

- 1. Access the system BIOS.
- 2. Select Advanced > AMD CBS > UMC Common Options > DDR Security.
- 3. Set **TSME** to either **Disabled** or **Auto**.

Chapter **D** 

# **Configuring SEV**

This chapter describes how to configure the Secure Encrypted Virtualization (SEV) feature.

# 3.1 AMD EPYC 9004 Series Processors

1. In BIOS, select **Advanced > AMD CBS > CPU Common Options**, and then set the **SEV Control** parameter to **Enable**.

Advanced	Aptio Setup -	AMI
Performance		<ul> <li>Can be used to disable SEV. To re-enable SEV, a POWER CYCLE is needed</li> </ul>
REP-MOV/STOS Streaming Prefetcher settings Core Watchdog	[Enabled]	after selecting the 'Enable' option.
RedirectForReturnDis	[Auto]	
Platform First Error Handling	(Auto)	
Core Performance Boost	[Auto]	
Global C-state Control	[Auto]	++: Select Screen
Power Supply Idle	[Auto]	11: Select Item
Control		Enter: Select
SEV-ES ASID Space	1	+/-: Change Opt.
Limit		F1: General Help
SEV Control	[Enable]	F2: Previous Values
Streaming Stores	(Auto)	F3: Optimized Defaults
Control		<ul> <li>F4: Save &amp; Exit</li> <li>ESC: Exit</li> </ul>

Figure 3-1: Setting SEV-ES Control to Enabled (AMD EPYC 9004 Series Processors)

2. Select Advanced > AMD CBS > CPU Common Options, and then change the SEV-ES ASID Count from Auto (1006) to 1006 or below to change the maximum number of ASIDs and the maximum amount of addressable DRAM. Set SEV-ES ASID Space Limit to the desired value based on the types of VMs you will be running. ASIDs less than 'x' are for SEV-ES, and ASIDs greater than or equal to 'x' are for SEV. For example, if 5 is input in the field, then there will be 4 available SEV-ES ASIDs and the rest will be SEV only. If the field is set to 1, then SEV-ES will be disabled because

there are no available ASIDs for SEV-ES.See the **minSEVSASID** question in <u>"Frequently Asked Questions" on page 37</u> for more detailed information.

REP-MOV/STOS Streaming Prefetcher settings Come Watchdog	(Enabled)	SEV-ES and SNP guests must use ASIDs in the range 1 through (this
RedirectForReturnDis	[Auto]	value -1). SEV guests
Platform First Error	(Auto)	must use ASIDs in the
Handling		range of this value
Core Performance Boost	[Auto]	through 1006. To have
Global C-state Control	[Auto]	all ASIDs support
Power Supply Idle	[Auto]	
Control		
SEV-ES ASID Space	123	+: Select Screen
CIMIT	(Feebla)	Fotos: Solost
Streaming Stores	(Endole)	Litter: Select
Control	(noto)	E1: General Hein
Local APIC Mode	[Auto]	F2: Previous Values
ACPI _CST C1	(Auto)	F3: Optimized Defaults
Declaration		▼ F4: Save & Exit
		ESC: Exit

Figure 3-2: Configuring SEV-ES ASID Space Limit (AMD EPYC 9004 Series Processors)

# **3.2 AMD EPYC 7003 and 7002 Series Processors**

To configure SEV on a system powered by an AMD EPYC 7003 or 7002 Series Processor:

 In BIOS, select Advanced > AMD CBS > CPU Common Options, and then set the SEV-ES ASID Space Limit Control parameter to Manual.

Aptio Setup — AMI Advanced			
Global C-state Control	(Auto)	▲ Customize SEV-ES ASID	
Power Supply Idle Control	[Auto]	space limit	
SEV ASID Count	[Auto]		
SEV-ES ASID Space			
Streaming Stores Control Local APIC Mode ACPI_CST C1 Declaration	[Auto] EV-ES ASID Space Limit	Control	
Streaming Stores Control Local APIC Mode ACPI _CST C1 Declaration MCA error thresh enable	LAUTOJ SV-ES ASID Space Limit	Control	
Streaming Stores Control Local APIC Mode ACPI _CST C1 Declaration MCA error thresh enable SMU and PSP Debug Mode	[Auto] SV-ES ASID Space Limit [Auto]	Control t Screen t Item Enter: Select +/-: Change Opt.	
Streaming Stores Control Local APIC Mode ACPI_CST C1 Declaration MCA error thresh enable SMU and PSP Debug Mode PPIN Opt-in	[Auto] SV-ES ASID Space Limit [ [Auto] [Auto]	Control t Screen t Item Enter: Select +/-: Change Opt. F1: General Help	
Streaming Stores Control SE Local APIC Mode ACPI _CST C1 Declaration MCA error thresh enable SMU and PSP Debug Mode PPIN Opt-in SNP Memory (RMP Table) Coverage	[Auto] SV-ES ASID Space Limit (Auto] [Auto] [Auto]	Control t Screen t Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults	

Figure 3-3: Setting SEV-ES Space Limit Control to Manual (AMD EPYC 7003 and 7002 Series Processors)

Chapter 3: Configuring SEV

2. Select Advanced > AMD CBS > CPU Common Options, and then change the SEV-ES ASID Count from Auto (509/253) to 509/253 or less to change the maximum number of ASIDs and the maximum amount of addressable DRAM. Set SEV-ES ASID Space Limit to the desired value based on the types of VMs you will be running. ASIDs less than 'x' are for SEV-ES, and ASIDs greater than or equal to 'x' are for SEV. For example, if 5 is input in the field, then there will be 4 available SEV-ES ASIDs and the rest will be SEV only. If the field is set to 1, then SEV-ES will be disabled because there are no available ASIDs for SEV-ES. See the minSEVSASID question in <u>"Frequently Asked Questions" on page 37</u> for more detailed information.

Note: If the system detects 8TB or more of DRAM, then BIOS will automatically switch this to 253 ASIDs.

Advanced	Hptio Setup – HMi	
Core Performance Boost	[Auto]	▲ SEV VMs using ASIDs
Global C-state Control	(Auto)	below the SEV-ES ASID
Power Supply Idle Control	[Auto]	Space Limit must enable the SEV-ES feature.
SEV ASID Count	[Auto]	ASIDS from SEV-ES ASID
SEV-ES ASID Space	(Manual)	Space Limit to (SEV
Limit Control		ASID Count + 1) can
SEV—ES ASID Space Limit	1	only be used with SEV
Streaming Stores	(Auto)	the Salact Scheen
Local APIC Mode	[Auto]	11: Select Item
ACPT CST C1	[Auto]	Enter: Select
Declaration	Lind Col	+/-: Change Opt.
MCA error thresh	[Auto]	F1: General Help
enable		F2: Previous Values
SMU and PSP Debug Mode	[Auto]	F3: Optimized Defaults
PPIN Opt-in	[Auto]	▼ F4: Save & Exit ESC: Exit

Figure 3-4: Configuring SEV-ES ASID Space Limit (AMD EPYC 7003 and 7002 Series Processors)

### **3.3 AMD EPYC 7001 Series Processors**

1. In BIOS, select Advanced > AMD CBS > CPU Common Options, and then set the SEV-ES ASID Space Limit Control parameter to Manual.

Advanced	Aptio Setup — AMI	
Global C-state Control	[Auto]	Customize SEV-ES ASID
Power Supply Idle	[Auto]	space limit
Control		
SEV ASID Count	[Auto]	
SEV-ES ASID Space		
Limit Control		
Streaming Stores	[Auto]	
Control SE	V—ES ASID Space Limit Cont	rol
Local APIC Mode Auto		
ACPI_CSICI Manual		4. 000000
MCA appon thresh		t Screen
enable		Enter: Select
SMU and PSP Debug Mode	[Auto]	+/-; Change Opt.
PPIN Opt-in	[Auto]	F1: General Help
SNP Memory (RMP	[Auto]	F2: Previous Values
Table) Coverage		F3: Optimized Defaults
SMEE	[Auto]	F4: Save & Exit
		ESC: Exit
Version	2.21.1278 Copyright (C) 2	022 AMI
		AB

Figure 3-5: Setting SEV-ES Space Limit Control to Manual

2. Set **SEV-ES ASID Space Limit (16)** to the desired value based on the types of VMs you will be running. ASIDs less than 'x' are for SEV-ES and ASIDs greater than or equal to 'x' are for SEV. See the **minSEVSASID** question in <u>"Frequently Asked Questions" on page 37</u> for more detailed information. AMD recommends leaving this setting at either **Auto** or **1**.

Advanced	Aptio Setup — AMI			
Cone Performance Boost	[Auto]	SEV VMe using ASTDe		
Global C-state Control	[Auto]	below the SEV-ES ASTD		
Power Supply Idle	[Auto]	Space Limit must enable		
Control	charces	the SEV-ES feature.		
SEV ASID Count	[Auto]	ASIDS from SEV-ES ASID		
SEV-ES ASID Space	[Manual]	Space Limit to (SEV		
Limit Control		ASID Count + 1) can		
SEV-ES ASID Space	1	only be used with SEV 🔻		
Limit				
Streaming Stores	[Auto]			
Control	122223	↔: Select Screen		
Local APIC Mode	[Auto]	↑↓: Select Item		
ACPI _CST C1	[Auto]	Enter: Select		
Declaration		+/-: Change Opt.		
MCA error thresh	[Auto]	F1: General Help		
enable		F2: Previous Values		
SMU and PSP Debug Mode	[Auto]	F3: Optimized Defaults		
PPIN Opt-in	[Auto]	F4: Save & Exit		
		ESC: EXIT		
Veneior	2 21 1278 Copupight (C) 2	122 AMT		
version 2.21.1278 copyright (C) 2022 AMI				

Figure 3-6: Configuring SEV-ES ASID Space Limit

Chapter

# **Enabling/Disabling SNP**

This chapter describes how to enable and disable the AMD Secure Nested Paging (SNP) feature. This only applies to AMD EPYC 7003 Series Processors and above.

# 4.1 Enabling SNP

To enable SNP:

1. Enable and configure SEV and SEV-ES, as described in <u>"Configuring SEV" on page 15</u>.

Note: SNP only works on ASIDs that are SEV-ES capable (below MinSEVASID).

- 2. In the system BIOS, select **Advanced > AMD CBS > CPU Common Options**.
- Change SNP Memory (RMP Table) Coverage from Auto (which means Disabled) to Enabled. This will reserve memory for SNP and create the RMP that covers all of memory. If needed, you can select Custom to set the RMP to not cover all of memory.

Note: This only required for Linux hosts. Microsoft hosts do not require this when using SEV-SNP under Hyper-V.

Advanced	Aptio Set	up – AMI	
Power Supply Idle	[Auto]	- E	Enabled = ENTIRE system
Control		n	nemory is covered.
SEV ASID Count	LAutoJ		
SEV-ES ASID Space	[Auto]		
Limit Control			
Streaming Stores	[Auto]		
Control		Yable) Coverag	ge
Local APIC Mode	Disabled		
ACPI _CST C1	Enabled		
Declaration	Custom		
MCA error thresh	Auto		t Screen
enable -			t Item
SMU and PSP Debug			lect
PPIN Opt-in	[Auto]		⊢∕–: Change Opt.
SNP Memory (RMP		F	F1: General Help
Table) Coverage		F	2: Previous Values
SMEE	[Auto]	F	3: Optimized Defaults
Action on BIST Fa	ilure [Auto]	T F	4: Save & Exit
		E	ESC: Exit
	Version 2.21.1278 Co	pyright (C) 202	22 AMI
			AE

Figure 4-1: Changing SNP Memory (RMP Table) Coverage

You can also do this using MSRs. Before enabling SNP, first zero the RMP memory, and then write the address of the memory into the MSRs.

- MSRC001\_0132 [RMP Base] (Core::X86::Msr::LS\_RMP\_BASE)
- MSRC001\_0133 [RMP End] (Core::X86::Msr::LS\_RMP\_END)
- Enable SNP by setting the following MSR to 1: MSRC001\_0010 [System Configuration] (Core::X86::Msr::SYS\_CFG) bit 25 VmplEn set to 1

Please see Sections 15.26.4 and 15.36.1 in Volume 2 of the AMD <u>Architecture Programmer's Manual</u> for more information on RMP programming.

Next, configure the IOMMU to disable the vIOMMU:

1. In BIOS, select Advanced > AMD CBS > NBIO Common Options.

Advanced	Aptio Setup – AMI	
NBIO Common Options		Enable/Disable IOMMU
IOMMU DMAr Support DRTM Virtual Device Support ACS Enable PCIE ARI Support PCIE ARI Enumeration	[Auto] [Auto] [Auto] [Auto] [Auto] [Auto]	
<ul> <li>PCLE Ten Bit Tag Support</li> <li>HD Audio Enable</li> <li>SMU Common Options</li> <li>NBID RAS Common Options</li> </ul>	(Auto)	→+: Select Screen f4: Select Item Enter: Select +/-: Change Opt.
Enable AER Cap Early Link Speed Hot Plug Handling mode	[Auto] [Auto] [Auto]	<ul> <li>F1: General Help</li> <li>F2: Previous Values</li> <li>F3: Optimized Defaults</li> <li>▼ F4: Save &amp; Exit</li> <li>ESC: Exit</li> </ul>
Versior	2.21.1278 Copyright (C)	2022 AMI AB

Figure 4-2: NBIO Common Options

2. Set SEV-SNP Support to Enabled (default is Disabled).

Advanced	Aptio Setup — AMI	
ACS Enable PCIE ARI Support PCIE ARI Enumeration PCIE Ten Bit Tag Support HD Audio Enable > SMU Common Options > NBID RAS Common Options Enable AFR Can	[Auto] [Auto] [Auto] [Auto] [Auto] SEV-SNP Support Disable	Enable or Disable SEV-SNP Support
Early Link Speed Hot Plug Handling mode Presence Detect Select mode Preferred IO Data Link Feature Cap CV test SEV-SNP Support SRIS	Enable [ [Auto] [Auto] [Auto] [Disable] [Auto]	<pre>+: Select Screen 4: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version	2.21.1278 Copyright (C) 2	022 AMI

Figure 4-3: Enabling SEV-SNP support

## 4.2 Disabling SNP

Do not enable the SecureNestedPagingEn MSR bit: MSRC001\_0010 [System Configuration] (Core::X86::Msr::SYS\_CFG) bit 24 via x86.

Note: The system BIOS will never enable SecureNestedPagingEn. It always must be enabled by x86.

AMD recommends to leaving **SNP Memory (RNP Table)** Coverage set to Auto/Disabled in the BIOS, but there is no harm in leaving it **Enabled** if the hypervisor eventually wants to enable SNP. Leaving SNP memory coverage enabled will only remove some usable memory from the system.

The RMPBase and RMPEnd settings do not matter because RMP protection is not in effect since the SYS\_CFG MSR for SecureNestedPagingEn (bit 24) is disabled.



This page intentionally left blank.





# **OS Requirements**

For SEV or SEV-ES, verify that your OS supports SEV as a hypervisor and/or SEV as a guest, as shown in the following tables.

*Note:* TSME is OS-independent and only needs enablement in the BIOS.

### 5.1 SEV

The following kernels/OS support SEV:

OS/KERNEL	HOST	GUEST
Linux 4.15		$\checkmark$
Linux 4.16		
RHEL 7.6		$\checkmark$
RHEL 8	$\checkmark$	$\checkmark$
Fedora 28	$\checkmark$	$\checkmark$
SLES 15	$\mathbf{\nabla}$	$\checkmark$
Ubuntu 18.04		$\overline{\mathbf{A}}$
Ubuntu 18.10	$\checkmark$	$\checkmark$
Oracle UEK 5	$\checkmark$	$\checkmark$

Table 5-1: SEV support

# 5.2 SEV-ES

The following kernels/OS support SEV-ES:

OS/KERNEL	HOST	GUEST
Linux 5.10		
Linux 5.11		

Table 5-2: SEV-ES support

# 5.3 SEV-SNP

The following kernels/OS support SEV-SNP:

OS/KERNEL	HOST	GUEST
Linux 5.19	in development	

Table 5-3: SEV-SNP support

The SNP firmware requires IOMMU security protection, and a special OS kernel is required that knows how to configure the IOMMU. IOMMU must be enabled in BIOS. You can then use development kernels until the SNP patches have been merged into the main Linux kernel. See <u>https://github.com/AMDESE/AMDSEV/blob/sev-snp-devel/stable-commits</u>.

Chapter

# **OS Enablement**

# 6.1 Checking SEV Enablement

Execute the following command to find all SEV kernel prompts:

\$ sudo dmesg | grep SEV

SEV: You should see either:

•

- [CCP VALUE] SEV supported
- [CCP VALUE] SEV supported: 'xxx' ASIDs

Note: Both are valid, depending on the kernel version.

- SEV-ES: You should see:
  - [CCP VALUE] SEV-ES supported: 'xxx' ASIDs

For example, when both SEV and SEV-ES are enabled::

```
root@ :~# dmesg | grep SEV
[ 14.886391] ccp 0000:47:00.1: SEV firmware update successful
[ 15.140921] ccp 0000:47:00.1: SEV API:1.51 build: 3
[ 15.229519] SEV supported: `xxx' ASIDs
[ 15.229520] SEV-SEC supported: `xxx' ASIDs
```

In the above example:

- The number before ASIDs is the number of available ASIDs for the given SEV feature. SEV-ES ASIDs are meant for both SEV-ES and SEV-SNP.
- If either of the prompts do not appear, then verify that SEV and SEV-ES have been correctly enabled in the system, as described in the previous chapters. If so, then you must enable SEV and SEV-ES in the kernel, as described in the following section.

# 6.2 Enabling SEV

If SEV still does not appear in the kernel message after enabling it in BIOS, then you might need to enable it at the kernel level. To enable SEV in the kernel:

 Append the following to the kernel command line options: kvm\_amd.sev=1 kvm\_amd.sev\_es=1

- 2. Update grub in the OS.
- 3. Reboot the machine. SEV should now be enabled in the host OS.
- 4. In any guest, check for enablement by executing the same command shown in <u>"Checking SEV Enablement" on page 25</u>:

```
root@localhost:~# dmesg|grep SEV
[ 0.145741] Memory Encryption Features active: SMD SEV SEV-ES
```

#### 6.2.1 Additional Resources

Please see the following resources for additional information:

- Kernel.org: <u>https://www.kernel.org/doc/html/v5.7/virt/kvm/amd-memory-encryption.html</u>
- RHEL: <a href="https://access.redhat.com/articles/4491591">https://access.redhat.com/articles/4491591</a>
- **Oracle:** <u>https://blogs.oracle.com/linux/post/using-amd-secure-memory-encryption-with-oracle-linux</u>
- SUSE: <u>https://documentation.suse.com/sles/15-SP1/html/SLES-amd-sev/index.html</u>

# 6.3 Enabling SEV-SNP

DISCLAIMER: As of February 2023, SNP is still not supported upstream. You can follow these steps to build a demo kernel and get a look at an early version of SNP.

To enable SEV-SNP at the host level:

- 1. Follow the procedure described in <u>"Enabling SEV" on page 25</u> to enable SEV.
- Verify that the current firmware installed is the newest available (1.54 at the time of publication) for SNPcompatible AMD EPYC 7003 or 9004 Series Processor. If needed, update the firmware as described in <u>"Updating SEV</u> <u>Firmware" on page 27</u>.
- 3. Follow the steps listed in <u>https://github.com/AMDESE/AMDSEV/tree/sev-snp-devel</u> to build and install newest SNP kernel.
- Execute the command described in <u>"Checking SEV Enablement" on page 25</u> to verify that SEV-SNP is enabled. For example:

[ 0.720169] SEV-SNP: RMP table physical address 0x00000003a00000 - 0x0000000568fffff [ 6.560584] ccp 0000:47.00.1: SEV firmware update successful [ 8.151665] ccp 0000:47.00.1: SEV API:1.51 build:3 [ 8.151674] ccp 0000:47.00.1: [ 8.161364] SEV supported: 410 ASIDs [ 8.161364] SEV-ES and SEV-SNP supported: 99 ASIDs Chapter

# **Updating SEV Firmware**

You should always use the latest SEV firmware supported by your BIOS to have the latest features and security protection. To update SEV firmware:

- 1. Update your system BIOS.
- 2. Execute the SEV DownloadFirmware (DLFW) command. See <u>"DownloadFirmware" on page 27</u>.
- 3. Execute the SNP DownloadFirmwareEX (DLFW\_EX) command. See <u>"DownloadFirmwareEX" on page 29</u>.

The DownloadFirmware and DownloadFirmwareEX commands replace the local copy of SEV in DRAM with the new image. Calling the next SEV command loads that new copy into SRAM and runs it. The BIOS copy remains in SpiRom; rebooting the system will run the older BIOS image until you execute these commands again to update to the latest version.

## 7.1 DownloadFirmware

The DownloadFirmware command allows system administrators to the version of SEV running on the platform without having to reboot the platform or update the BIOS, provided that:

- All SEV/SNP guests are shut down.
- The SEV/SNP platform state is UNINIT.

The Linux CCP driver will automatically check for a new SEV image when initialized. If it finds a new image, then it will execute the DownloadFirmware command.

- 1. Download the latest firmware version from <a href="https://developer.amd.com/sev/">https://developer.amd.com/sev/</a>.
- 2. Check the /lib/firmware/amd/ directory to determine the system firmware format (.sbin or .esbin).
- 3. Copy the appropriate firmware filw (.sbin or .esbin) to /lib/firmware/amd/, and then name the file amd\_sev\_fam[ family ]h\_model[ model ]h.sbin Or amd\_sev\_fam[ family ]h\_model[ model ]h.esbin (see Figure 5-1). If needed, you may create an /amd folder, as shown in Figure 5-2, then paste the .sbin/ .esbin into this folder (see Figure 5-3), and then rename the firmware file as shown in Figure 5-4.

amd_sev_ram19del0xh_1.33.03	8 P.
amd_sev_ amd_sev_ Mili fam19h_ fam19h_ Rele model0xh_ model0xh_ Not 1.33.03. 1.33.03. ecbin sbin	tilan lease otes

Figure 7-1: Firmware download example

<	> I 🖸 lib f	irmware 🕨										c	ર := ≡	• • •
0														
ŵ														
		3com	acenic	adaptec	advansys	amdgpu	amd-ucode	ar3k	asihpi	ath6k	ath9k_htc	ath10k	atmel	
۵	Documents			_		_	_			_			_	
∻	Downloads													
99		atusb	av7110	bnx2	bnx2x	brcm	carl9170fw	cavium	cis	cpia2	cxgb3	cxgb4	dsp56k	
۵														
-														
Û		e100	ea	edgeport	emi26	emi62	ene-ub6250	ess	go7007	hp	i915	imx	intel	
+	Other Locations													
		intel-ucode	isci	kaweth	keyspan	keyspan_pda	korg	libertas	liquidio	matrox	mediatek	mellanox	moxa	
					-			_						
		mrvl	mwl8k	mwlwifi	netronome	nvidia	ositech	qca	qcom	qed	qlogic	r128	radeon	
		rockchip	rsi	RTL8192E	rtl_bt	rtl_nic	rtlwifi	rtw88	sb16	scripts	slicoss	sun	tehuti	
													1 10 101 1010	
		ti-connectivity	tigon	ti-keystone	ttusb-budget	ueagle-atm	usbdux	vicam	vxge	yam	yamaha	zd1211	1a98-INTEL- EDK2-2-tplg. bin	
		1 10 101 1010	THE REAL PROPERTY.	1 10 101 1010	1 10 101 1010	1 10 101 1010			1 10 101 1010	1 10 101 1010	1 10 101 1010	1 10 101 1010	1 10 101 1010	
		a300_pfp.fw	a300_pm4.fw	agere_ap_fw. bin	agere_sta_fw. bin	ar5523.bin	as 102_data 1_ st.hex	as102_data2_ st.hex	ath3k-1.fw	atmel_ at76c504_ 2958.bin	atmel_ at76c504a_ 2958.bin	atmsar11.fw	carl917 <b>0-1.f</b> w	
												E D	E D	

*Figure 7-2: lib\_firmware folder, with the /amd subfolder created.* 

lib	firmware	amd	<b>&gt;</b>	۹	:=	=	008
	amd_sev_ fam19h_ nodel0xh_ .33.03.sbin			1			

Figure 7-3: Pasted .sbin before renaming



Figure 7-4: Pasted .sbin after renaming



You can find the latest SEV firmware images at <u>https://developer.amd.com/sev/</u>. See Figure 5-5.

**Technical Presentations** 

Figure 7-5: SEV firmware download links

AMD EPYC 7002 Series Processors and newer always support SEV. AMD EPYC 7001 Series Processors require SEV firmware version 0.16 or above to run SEV. Please see the <u>SEV Specification</u> for additional information.

### 7.2 DownloadFirmwareEX

The DownloadFirmwareEX command only applies to 3rd Gen AMD EPYC processors and later. This command allows system administrators to the version of SEV running on the platform without having to reboot the platform or update the BIOS. SNP guests may remain running during the update, but all SEV guests must be shut down. The exception is that you may be required to shut down the guests or or uninitialize the SNP platform in certain cases, such as if a security bug was found in a previous version and the running guests cannot be upgraded securely.

The minimum version requirements for this command are:

- **PSP Bootloader:** 00.13.00.60 (Milan PI 1004 BIOS).
- SEV uapp version: 1.2B.2B (around Milan PI 1007 BIOS).

If you are running a SEV version that does not support DLFW\_EX, then you will have to first shut down your guests and then call the regular DLFW command (see <u>"DownloadFirmware" on page 27</u>) to upgrade to the SEV version that supports DownloadFirmwareEX and then use DownloadFirmwareEX going forward.

Please see the <u>SEV Specification</u> for additional information.



This page intentionally left blank.

Chapter

# Launching an Encrypted VM

# 8.1 Launching a VM with SEV Encryption

To launch a VM with SEV encryption, enable SEV in the system as described in <u>"Enabling SEV" on page 25</u>, and then verify that you have the following minimum versions:

PROJECT	VERSION
Libvert	4.5
QEMU	2.12
OVMF	Commit newer than (75b7aa9528bd 2018-07-06)

Table 8-1: Minimum project versions to support SEV-encrypted VMs

### 8.1.1 Launching with QEMU

In the desired launch directory:

- 1. Create a new qcow2 image: \$ qemu-img create -f qcow2 encryptedImage.qcow2 30G
- 2. Copy the OVMF\_VARS.fd file: \$cp /usr/share/OVMF/OVMF\_VARS.fd OVMF\_VARS.fd
- 3. Launch your VM using your desired ISO image and the following commands as a minimum: \$ gemu-system-x86 64 \

```
-enable-kvm \
-cpu EPYC \
-machine q35 \
-no-reboot \
-vga std \
-vrc :0
-drive file=distro.iso=cdrom -boot d \
-drive if=pflash,format=raw,unit=0,file=/usr/share/OVMF/OVMF_CODE.fd,readonly=on \
-drive if=pflash,format=raw,unit=1,file=OVMF_VARS.fd \
-drive file=encryptedImage.qcow2,if=none,id=disk0,format=qcow2
-device virtio-scsi-pci,id=scsi0,disable-legacy=on,iommu_platform=on
-device scsi-hd,drive=disk0
-machine memory-encryption=sev0,vmport=off
-object sev-quest,id=sev0,policy=0x3,cbitpos=47,reduced-phys-bits=1
```

In the preceding example, the cbitpos parameter in the line - object sev-

guest,id=sev0,policy=0x3,cbitpos=47,reduced-phys-bits=1 changes depending on the processor
generation. AMD EPYC 7002 and 7001 Series Processors have a c-bit value of 47, and AMD EPYC 7003 Series Processors
and newer have a c-bit value of 51.

If you are not sure what the appropriate cbit is, then you may check the EBX register on the **0x8000001f** CPUID function by executing the CPUID command:

\$ cpuid -r -1 0x8000001f I

In this example:

- The bits 0-5 make up the appropriate cbit value.
- EBX is a hex number; you may need a conversion to find this value. amdsev@amdsev:~\$ cpuid -r -l -l 0x8000001f CPU: 0x8000001f 0x00: eax=0x0101fd3f ebx=0x00004173 ecx=0x000001fd edx=0x00000064

Note: You may need to edit these commands to suit your particular needs and use cases. For example, different distros may have different QEMU launch commands. Please see the guides listed in <u>"Additional Resources" on page 26</u> for more information.

- 4. Launch the VM, and then install the distro. You can now launch the VM using the qcow2 image without using the ISO.
- 5. On the guest, execute the dmesg | grep SEV command to verify that SEV is enabled. root@localphost:!# dmesg | grep SEV [ 0.150352] Memory ENcryption Features active: AMD SEV

### 8.1.2 Launching with Libvirt

Please see <u>https://libvirt.org/kbase/launch\_security\_sev.html</u> for instructions on launching encrypted VMs with Libvirt.

# 8.2 Launching a VM with SEV-ES Encryption

To launch a VM with SEV-ES encryption, enable SEV in the system as described in <u>"Enabling SEV" on page 25</u>, and then verify that you have the following minimum versions:

PROJECT	VERSION
Libvert	4.5
QEMU	6.0
OVMF	Commit newer than (EDK2-STABLE 2020-21-02)

Table 8-2: Minimum project versions to support SEV-encrypted VMs

1. If needed, install the correct versions.

Chapter 8: Launching an Encrypted VM

 Execute the launch command, which is very similar to the command used for <u>"Launching a VM with SEV Encryption"</u> on page 31, except for the following line:

-object sev-guest, id=sev0, policy=0x3, cbitpos=47, reduced-phys-bits=1, where the policy variable should be changed to reflect SEV-ES enablement, as shown in the following table:

OFFSET	BIT(S)	NAME	DESCRIPTION	
000h	0	NODBG	Debugging of the guest is disallowed when set.	
	1	NOKS	Sharing keys with other guests is disallowed when st.	
	2	ES	SEV-ES is required when set.	
	3	NOSEND	Sending the guest to another platform is disallowed when set.	
	4	DOMAIN	The guest must not be transmitted to another platform that is not in the domain when set.	
	5	SEV	The guest must not be transmitted to another platform that is not SEV-capable when set.	
	15:6		Reserved; should be 0.	
002h	7:0	API_MAJOR	The guest must not be transmitted to another platform with a lower	
003h	7:0	API_MINOR	firmware version.	

Table 8-3: SEV policy bits

As shown in the previous table:

- The policy bit 2 must be set to launch SEV-ES. The policy is passed as a hexadecimal number.
- A valid SEV-ES configuration would look like this: -object sev-guest, id=sev0, policy=0x5, cbitpos=47, reduced-phys-bits=1
- Everything else is the same as SEV.
- On the guest, execute the command dmesg | grep SEV to confirm SEV-ES enablement.

# 8.3 Launching a VM with SEV-SNP Encryption

As of publication, SEV-SNP does not yet have upstream QEMU or OVMF patches. The guest kernel is currently the only item with upstream support. See <u>"OS Enablement" on page 25</u> for version information. You can build SNP-compatible OVMF and QEMU at <u>https://github.com/AMDESE/AMDSEV/tree/sev-snp-devel</u>.

Build the correct OVMF and QEMU, and then launch an SNP guest by executing a command similar to that used for regular SEV:

```
$ PATH-TO-SNP-QEMU/qemu-system-x86_64 \
-enable-kvm \
-cpu EPYC \
-machine q35 \
-no-reboot \
-vga std \
-vnc :0\
-drive if=pflash,format=raw,unit=0,file=PATH-TO-SNP-OVMF/OVMF_CODE.fd,readonly=on \
-drive if=pflash,format=raw,unit=1,file=OVMF_VARS.fd \ <- make sure you copy this file from
build ovmf
-drive file=SNPGUEST.qcow2,if=none,id=disk0,format=qcow2 \
-device virtio-scsi-pci,id=scsi0,disable-legacy=on,iommu platform=on \</pre>
```



-device scsi-hd,drive=disk0 \
-machine memory-encryption=sev0,vmport=off \
-object sev-snp-guest,id=sev0,cbitpos=51,reduced-phys-bits=1

This command should allow you to launch an SNP-enabled VM if your guest has the correct kernel. You can execute the command dmesg | grep SEV on the guest to confirm that SNP is launched:

root@localhost:~# dmesg | grep SEV [ 0.150352] Memory Encryption Features avcoe: AMD SEV SEV-ES SEV-SNP

Note: LibVirt currently does not support SNP.



# **Confidential Containers**

SEV is now supported on confidential containers via an open-source that allows you to launch SEV encrypted katacontainers. Please visit <u>https://github.com/confidential-containers/documentation/blob/main/quickstart.md</u> for information and instructions on how to set-up confidential containers.



This page intentionally left blank.

Chapter

# **Frequently Asked Questions**

#### What is MinSEVASID?

MinSEVAsid is the minimum ASID that lets you run SEV guests, everything below that is for SEV-ES and SEV-SNP guests. For example, if MinSEVAsid is set to 8, then ASIDs 1-7 can only be assigned to SEV-ES or SEV-SNP guests, and ASIDs 8-(max) can only be used for SEV guests.

#### How do I map more than 8TB/16TB of physical address space?

To map to more than 8TB of physical address space (DRAM + PCIe + MMIO, etc), change **SEV ASID Count** to 253 in the BIOS. AMD EPYC 7003 and 7002 AGESA will automatically change this setting to 253 if more than 8TB of physical address space is detected during boot. You must disable SME (which also disables SEV) to map to more than 16TB of physical address space. See <u>"Disabling SMEE in BIOS" on page 9</u>.

#### How many bits are being used by ASIDs and where is the C-bit on my generation of platform?

See <u>"Disabling SMEE via MSR" on page 10</u> to find the number of bits being used by ASIDs.

- 1st and 2nd Gen AMD EPYC processors have the c-bit in bit 47.
- 3rd and 4th Gen AMD EPYC processors have the c-bit in bit 51.

If in doubt, check CPUID\_Fn8000001F\_EBX [AMD Secure Encryption EBX] (Core::X86::Cpuid::SecureEncryptionEbx) to find the c-bit position. See <u>"Launching a VM with SEV</u> Encryption" on page 31 for additional information.

3rd and 2nd Gen AMD EPYC with 256 ASIDs (8 bits) and 16TB DRAM	3rd and 2nd Gen AMD EPYC with 512 ASIDs (9 bits) and 8TB DRAM			
64:52 reserved	64:52 reserved			
51:44 asids/cbit cbit=51	51:43 asids/cbit cbit=51			
43:0 PhysAddr	42:0 PhysAddr			

Table 10-1: ASID bit usage

#### Where is the SEV documentation?

See <a href="https://developer.amd.com/sev/">https://developer.amd.com/sev/</a>.

#### Does the APM vol 2 support SEV and SNP?

Yes. See <u>https://www.amd.com/system/files/TechDocs/24593.pdf</u>.

#### What is SEV 2?

This is not an official AMD term but may refer to the second implementation of SEV (on 2nd Gen AMD EPYC processors that have 509 ASID keys).

#### I have questions about PCDs

Please contact the AMD BIOS support team. The firmware team does not know about PCDs. The BIOS documentation on SEV-related options should be good enough on its own or will need to be updated.

#### How big will my RMP be for a given amount of memory?

Each RMP entry is 16 bytes, and 256 RMP entries can fit in a 4K page. So, for 512 GB of DRAM:

- 512\*1024\*1024\*1024 bytes / 4096 = 134,217,728 4K pages
- 134,217,728 4K pages \* 16 Bytes per RMP entry = 2,147,483,648 Bytes for all RMP entries
- 2,147,483,648 Bytes for all RMP entries / (1024\*1024) = 2,048 MB = 2GB (approx.)

#### How do I disable SEV?

The easiest way is to disable SMEE in the BIOS (see <u>"Disabling SMEE in BIOS" on page 9</u>). If you want to still use SME but not SEV, then you can blacklist the <u>ccp</u> kernel driver so it doesn't load SEV. The last option is to remove the SEV binary from the BIOS, but that is not recommended.

#### How do I disable SNP?

Don't reserve memory for the RMP in the BIOS, and don't set the SNP\_EN MSR from x86. See <u>"Enabling/Disabling SNP"</u> on page 19 for more information.

#### Can we request new security features in later-generation AMD EPYC processors or to SEV?

The SEV spec is generally thought to be final, except for any security issues. Any new features will go into SNP.

#### How do I check if TSME is enabled?

You can check the kernel message to see if TSME is enabled by executing the command dmesg | grep SME, which should return a message similar to AMD Memory Encryption Features active: SME.

Additionally, a SNP guest can send a MSG\_REPORT\_REQ guest message to the PSP to get the SNP attestation report. Bit 1 (tsme\_en) of the PLATFORM\_INFO field contains the tsme\_en info.



#### Which version of SEV firmware did 'x' support get added?

	Feature	SEV Firmware Version
•	DownloadFirmware	0.16
•	GetID	
•	ActivateEX	0.18
•	Enhanced DownloadFirmware (PSP firmware dependency checking)	
•	InitEX	
•	SwapIn/SwapOut	0.23
•	NOP	
•	SendCancel	
•	Attestation	
RingBuffer		0.24

Table 10-2: SEV firmware versions with 'x' support



This page intentionally left blank.





# **Performance Data**

Please see Application Note: AMD SEVSNP Workloads Performance And Best Practices for AMD EPYC<sup>™</sup> 7003 Series Processors (login required) for information about SEV performance.



This page intentionally left blank.