Lenovo Configuration Guide for Confidential Computing and Microsoft CVM

Published: August 2026

Includes detailed steps for configuring Confidential Computing for AMD-Based Systems

Provides all details for all required UEFI settings

Dave Feisthammel
Andreina Vivas Thomas
David Ye

LENOVO PRESS

Abstract

Confidential Computing is a groundbreaking security technology that protects data in use by performing computations in a hardware-based, isolated Trusted Execution Environment (TEE). While traditional security measures protect data at rest (in storage) and data in transit (across networks), data remains vulnerable when it is actively processed in memory. As organizations increasingly migrate sensitive workloads to multi-tenant cloud environments and embrace collaborative AI, securing data during runtime has become a critical business imperative.

This white paper explains how to configure Lenovo ThinkAgile MX server firmware settings to support Microsoft's implementation of Confidential Virtual Machines (CVM). At the time of this writing, CVM only supports AMD platforms. We use the ThinkAgile MX455 V3 server for examples throughout this paper.

Do you have the latest version? Check whether you have the latest version of this document by clicking the **Check for Updates** button on the front page of the PDF. Pressing this button will take you to a web page that will tell you if you are reading the latest version of the document and give you a link to the latest if needed. While you're there, you can also sign up to get notified via email whenever we make an update.

Contents

Introduction

Confidential Computing is a groundbreaking security technology that protects data in use by performing computations in a hardware-based, isolated Trusted Execution Environment (TEE). While traditional security measures protect data at rest (in storage) and data in transit (across networks), data remains vulnerable when it is actively processed in memory. As organizations increasingly migrate sensitive workloads to multi-tenant cloud environments and embrace collaborative AI, securing data during runtime has become a critical business imperative.

This introduction explores how Confidential Computing fills the final gap in data encryption, enabling zero-trust cloud computing, secure multi-party collaboration, and robust regulatory compliance.

The Runtime Security Gap

Traditional enterprise security frameworks successfully protect data in two of its three primary states. Data at rest is secured via storage encryption, and data in transit is protected using cryptographic network protocols like TLS.

However, a critical vulnerability remains; data in use. To process data, a CPU must decrypt it into system memory (RAM). During execution this plain text data is exposed to:

- Unprivileged system administrators.
- Malicious insiders with physical or root access.
- Compromised host operating systems or hypervisors.
- Advanced memory-dumping malware and side-channel exploits.

Confidential Computing addresses this fundamental flaw. It extends encryption into the processor itself, completing the lifecycle of end-to-end data protection.

Hardware-Based Isolation: The TEE

The core mechanism of Confidential Computing is the Trusted Execution Environment (TEE), often referred to as a hardware enclave. TEEs are isolated memory regions enforced directly at the silicon level by modern CPUs (e.g., AMD SEV-SNP)

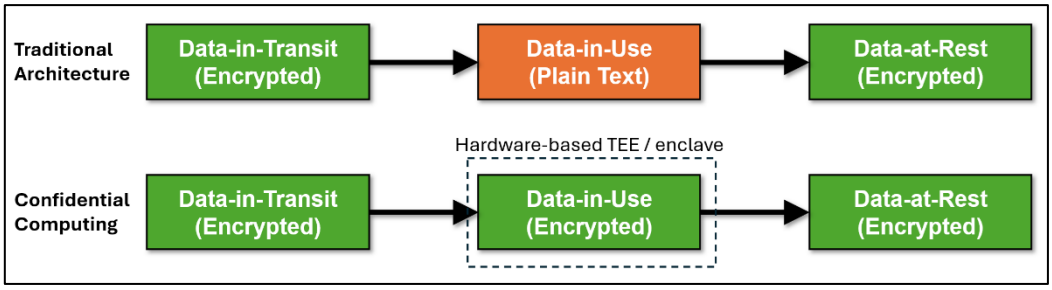

Figure 1: Confidential computing vs. traditional architecture

When an application runs inside a TEE:

- Memory Encryption: The CPU transparently encrypts the enclave's memory pages using hardware-managed keys.
- Access Control: Any access attempt by the host operating system, hypervisor, or peer virtual machines is blocked at the hardware level.
- Cryptographic Attestation: The CPU generates a signed hardware report proving that the exact, untampered application code was loaded securely inside a genuine TEE.

Engineering Drivers for Implementation

For infrastructure, DevOps, and security engineers, implementing Confidential Computing satisfies three non-negotiable operational requirements:

- True Zero-Trust Architecture: Engineers can treat the underlying cloud provider, host infrastructure, and virtualization layers as completely untrusted. You own the data keys; the platform provider cannot inspect your code or state.
- Secure Multi-Party Computation (SMPC): It enables data sharing and collaborative analytics (such as joint machine learning training) with external partners without ever exposing raw datasets to the other parties.
- De-risking Cloud Migration: High-risk workloads—such as cryptographic key management, financial transaction processing, and proprietary AI models—can be safely lifted and shifted to public, multi-tenant cloud environments.

Confidential Computing is supported by Microsoft as “Confidential VMs” (CVM), which provide strong isolation boundaries by extending data protection from storage and networks directly into the hardware. CVMs use hardware-based Trusted Execution Environments (TEEs) to make a virtual machine's runtime memory completely opaque to the underlying infrastructure.

For additional information regarding Confidential Computing and Confidential VMs from Microsoft, refer to the following article:

https://azure.microsoft.com/en-us/solutions/confidential-compute

Configure UEFI settings

To enable SEV-SNP the following UEFI settings must be configured:

AMD Secure Memory Encryption (SME)

This setting must be set to Enabled.

Path: UEFI Settings → System Settings → Memory → SMEE → Enabled

Description: This setting is required to use all Secure Encrypted Virtualization features and uses a single key to encrypt system memory and provides additional security benefits. For example, when enabled it can protect the Hypervisor and the Host OS.

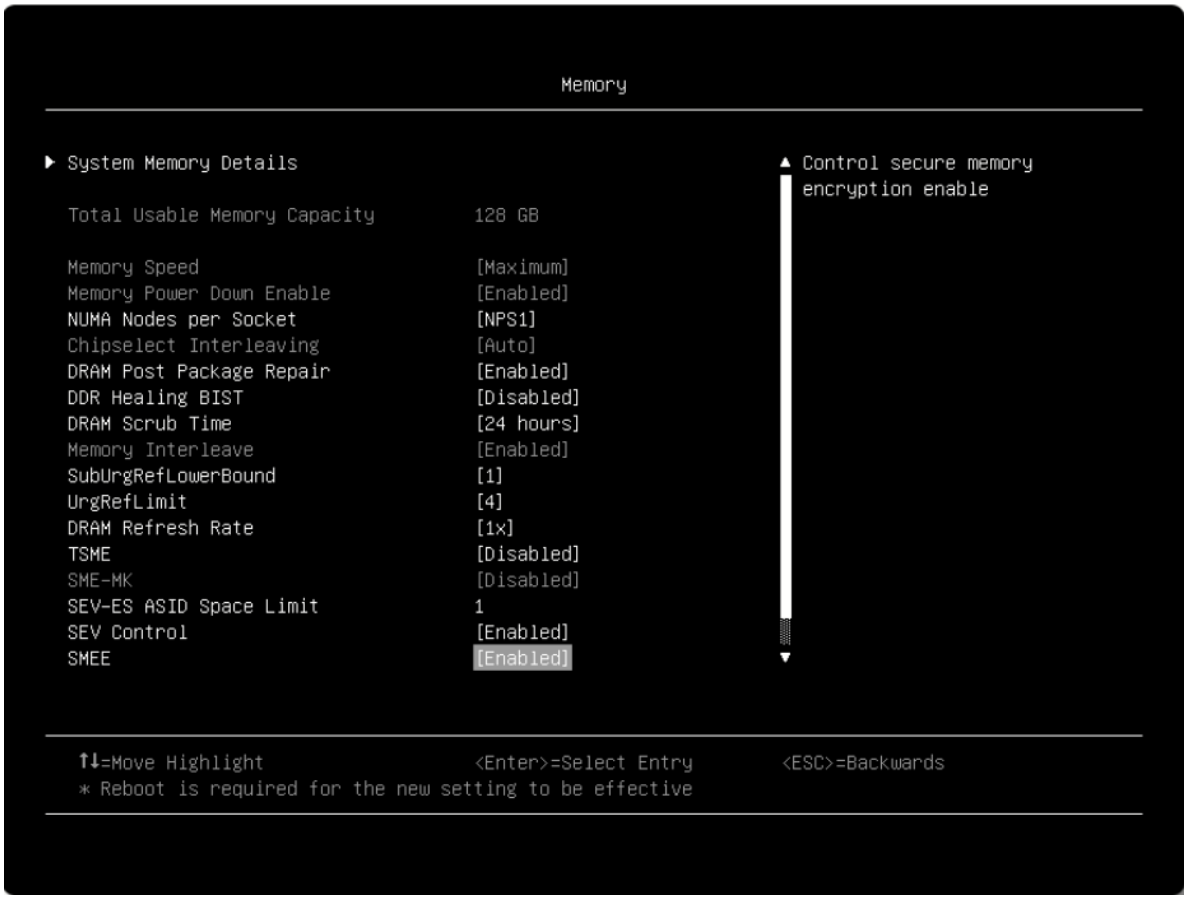

Figure 2: System Setup screen showing the SMEE setting

Transparent Secure Memory Encryption (TSME)

This setting must be set to Enabled.

Path: UEFI Settings → System Settings → Memory → TSME → Enabled

Description: When enabled, it provides full memory encryption without requiring changes to the operating system or applications. It is a simplified version of AMD Secure Memory Encryption. TSME is required for DRTM.

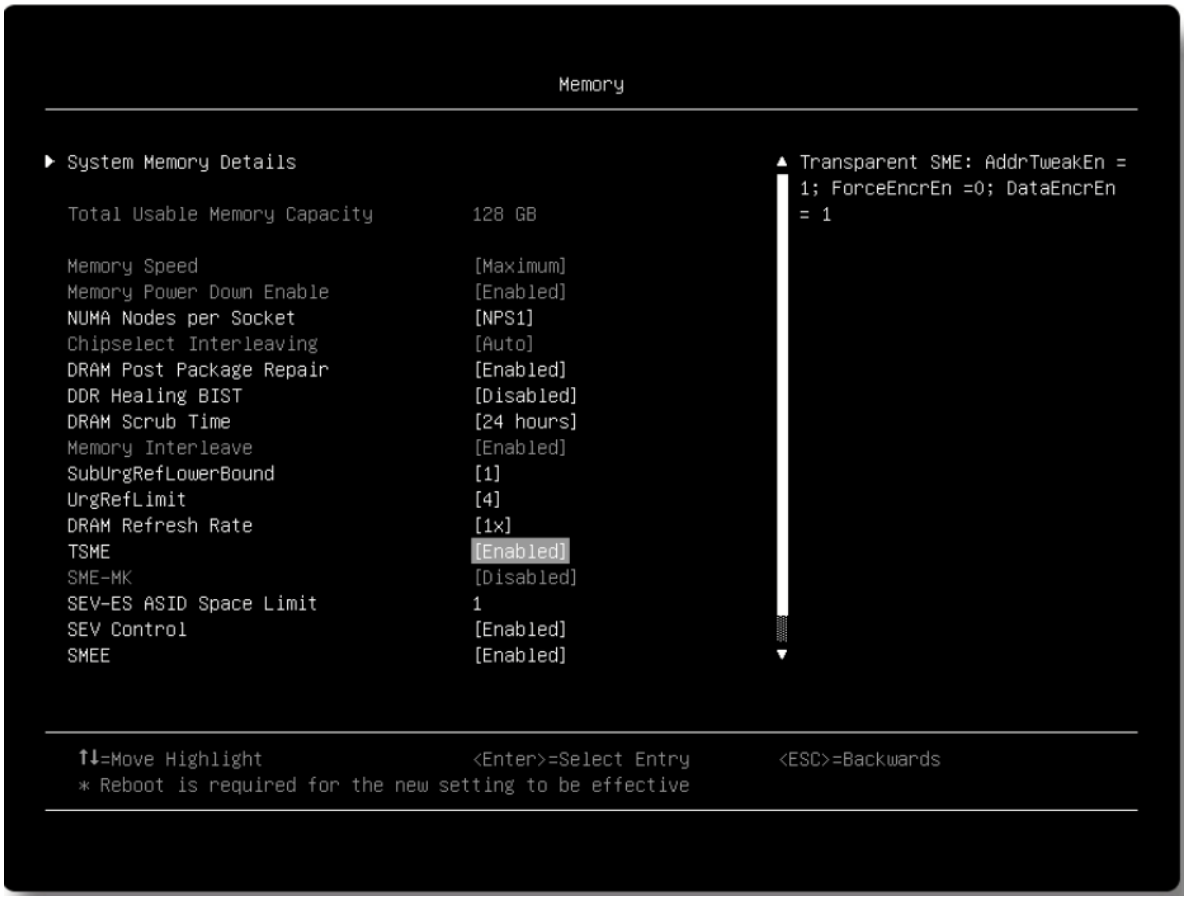

Figure 3: System Setup screen showing the TSME setting

Secure Encrypted Virtualization Address Space Identifier (ASID) Space Limit

Set this value to “ASID Count +1”

SEV-ES virtual machines are the most secure virtual machines.

Path: UEFI Settings → System Settings → Memory → SEV-ES ASID Space Limit → value

Description: SEV VMs using ASIDs below the SEV-ES ASID Space Limit must enable the SEV-ES feature. ASIDs from the SEV-ES ASID Space Limit to (SEV ASID Count + 1) can only be used with SEV VMs. If this field is set to (SEV ASID Count + 1), all ASIDs are forced to be SEV-ES ASIDs.

Figure 4: System Setup screen showing the SEV-ES ASID Space Limit setting

Secure Encrypted Virtualization Control

This setting must be set to Enabled.

Path: UEFI Settings → System Settings → Memory → SEV Control → Enabled

Description: This setting enables SEV control. Enables confidential computing by protecting VM memory and state from unauthorized access.

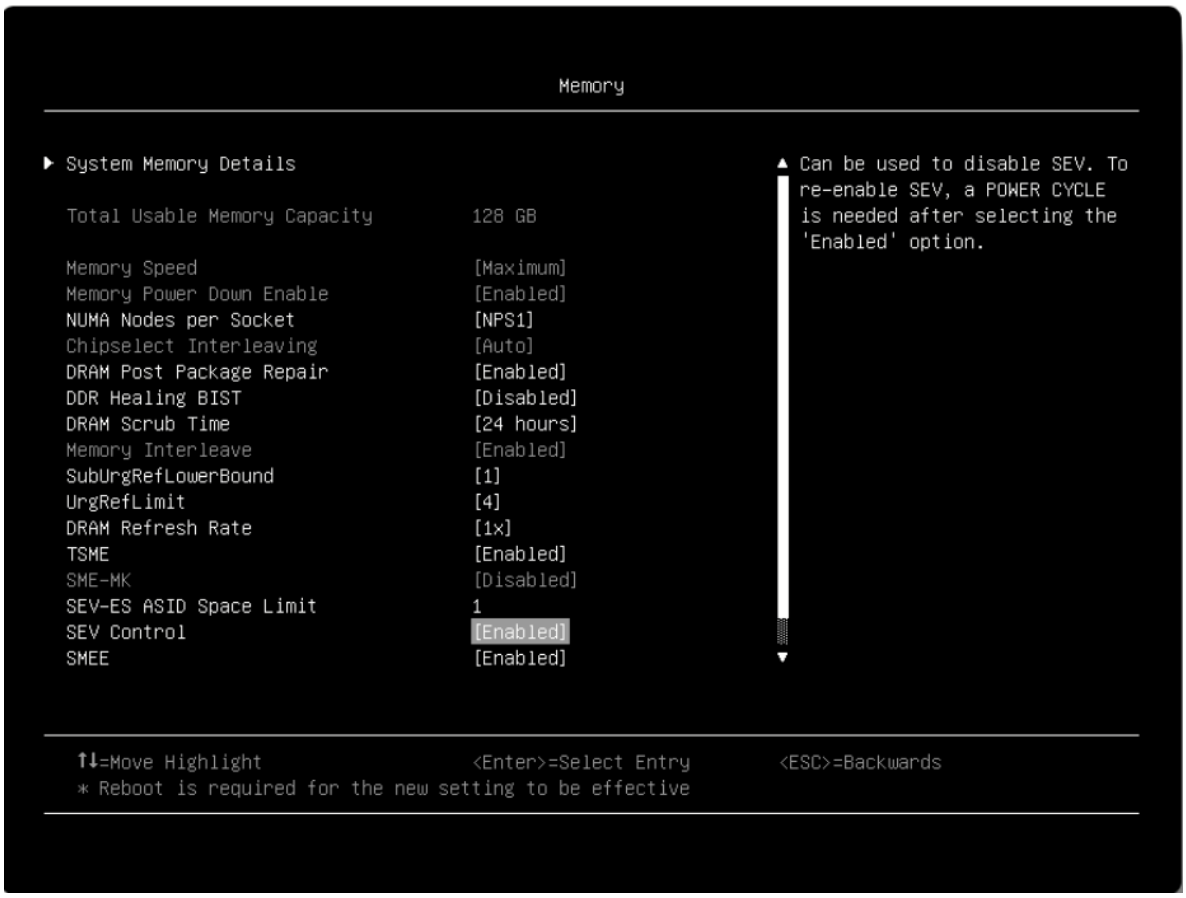

Figure 5: System Setup screen showing the SEV Control setting

SVM Mode

This setting must be set to Enabled.

Path: UEFI Settings → System Settings → Processors → SVM Mode → Enabled

Description: This setting enables CPU Virtualization. Enables Secure Virtual Machine Mode and is required for SEV-ES and SEV-SNP and for Confidential Computing features.

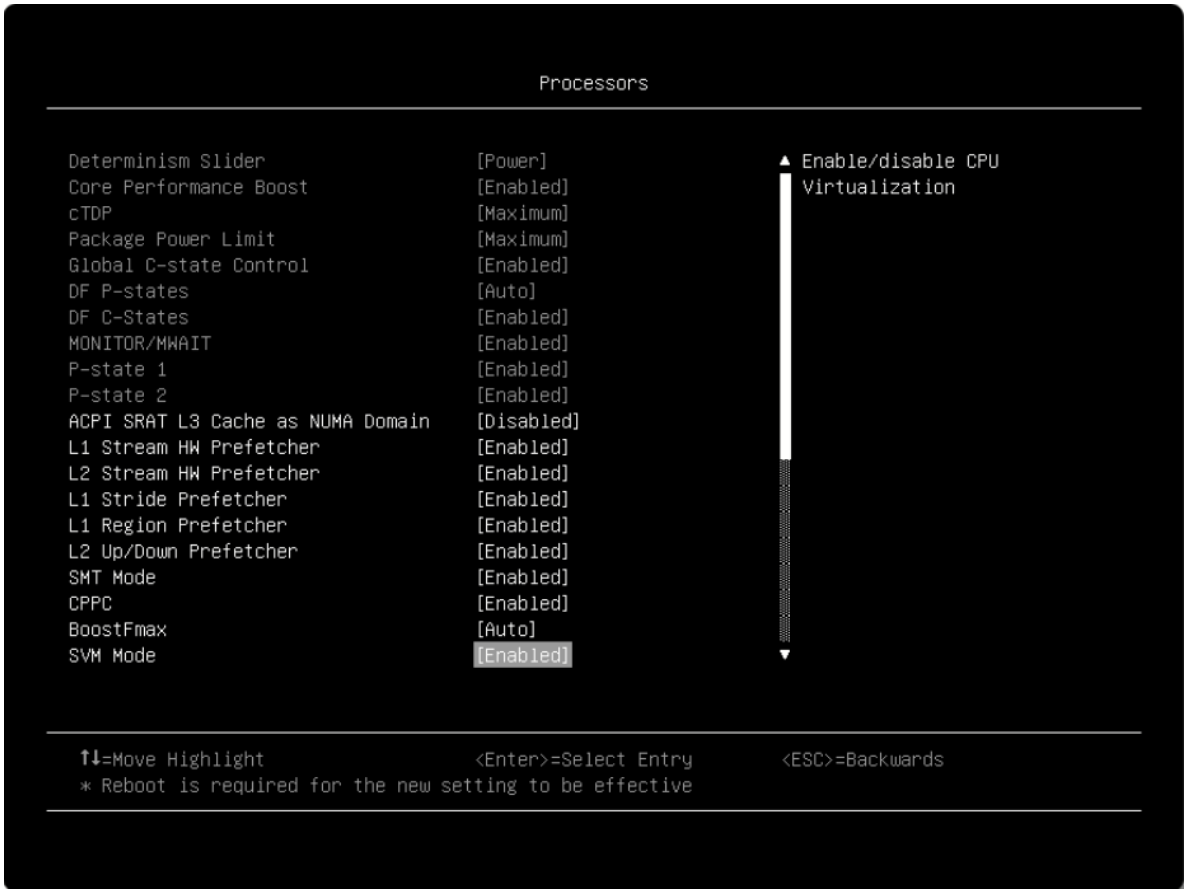

Figure 6: System Setup screen showing the SVM Mode setting

Secure Encrypted Virtualization-Secure Nested Paging (SNP)

This setting must be set to Enabled.

Path: UEFI Settings → System Settings → Processors → SEV-SNP Support → Enabled

Description: This setting enables SEV-SNP support. Provides memory integrity protection and guest isolation from the hypervisor.

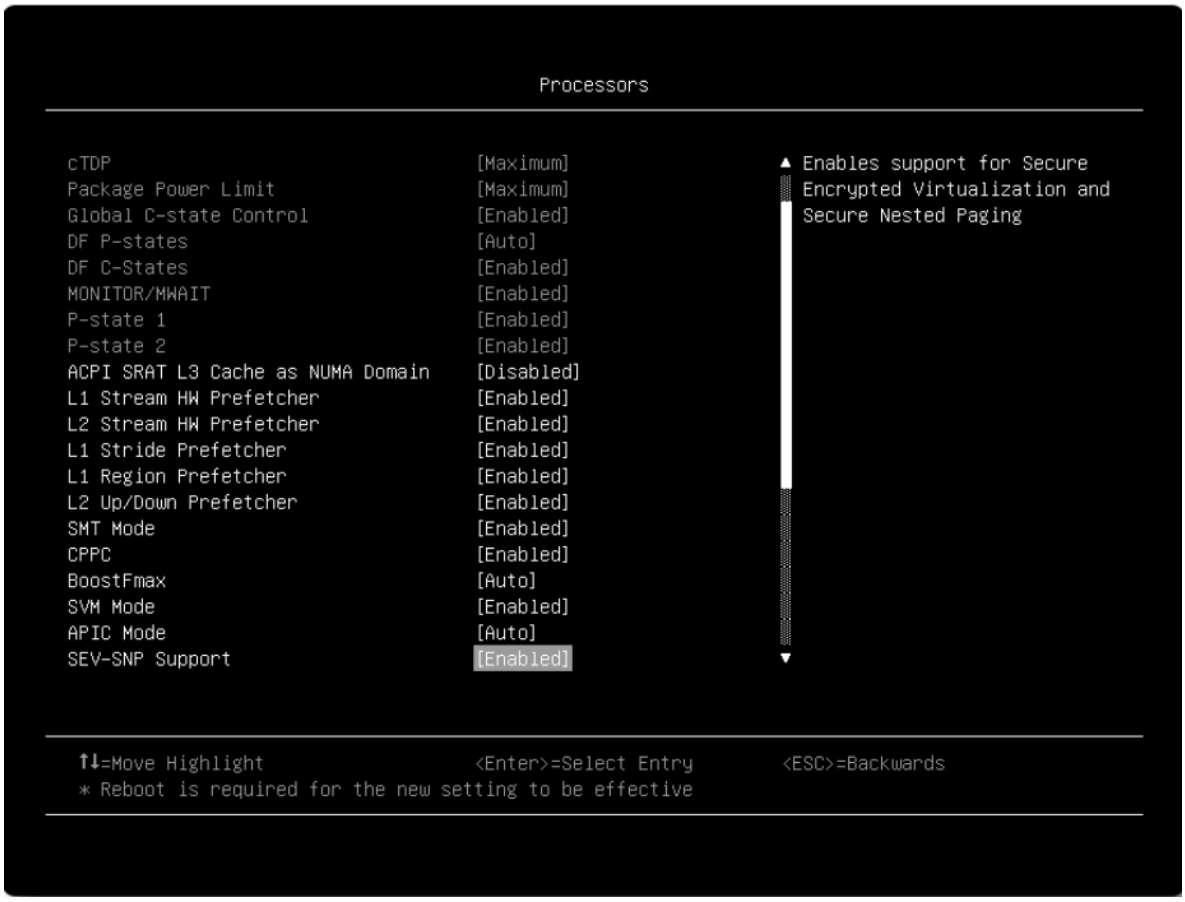

Figure 7: System Setup screen showing the Secure Encrypted Virtualization SNP Support setting

Secure Nested Paging (SNP) RMP Table Coverage

This setting must be set to Disabled.

Path: UEFI Settings → System Settings → Processors → SNP Memory (RMP Table Coverage) → Disabled

Description: The use of the Reverse Map Table (RMP) Table to protect memory when SEV-SNP is enabled. This is not applicable to Hyper-V as it allocates and manages its own RMP table instead of platform firmware

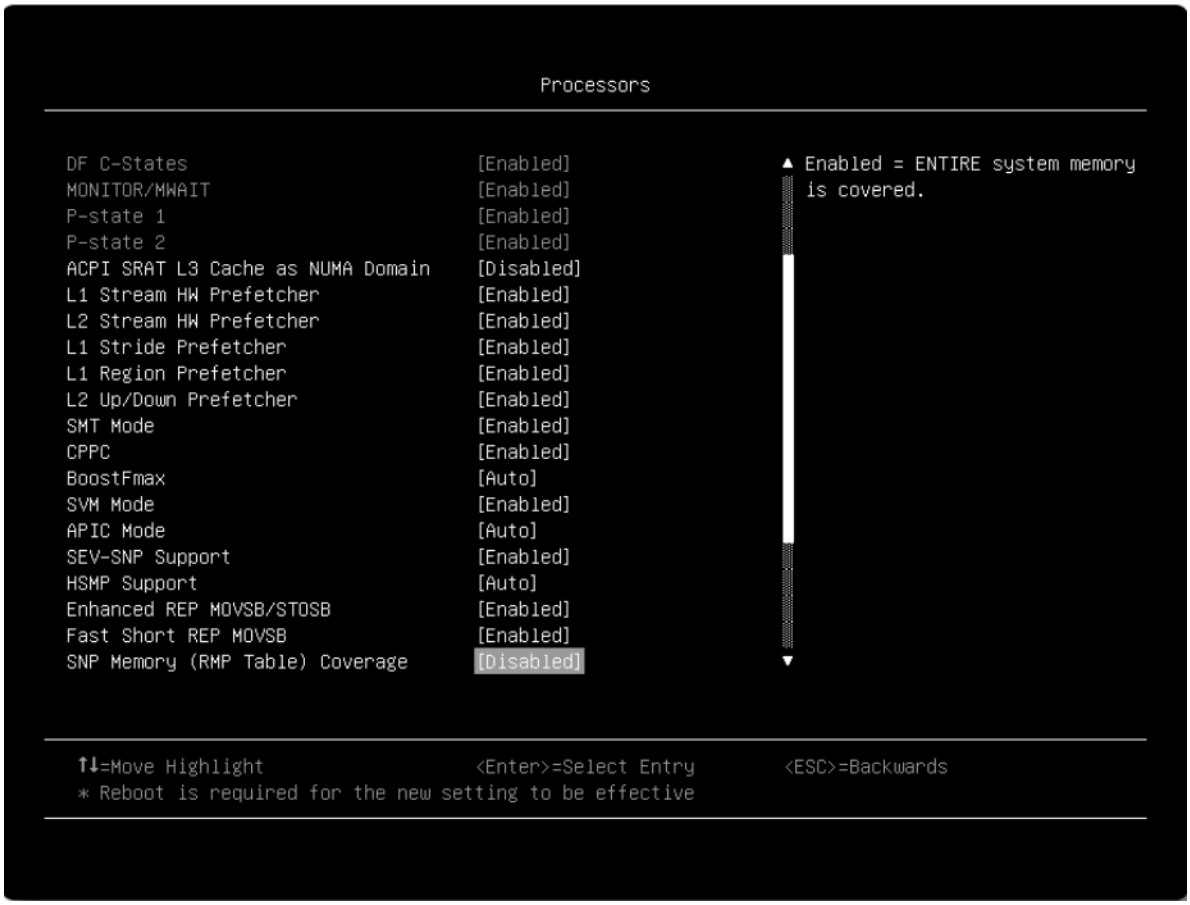

Figure 8: System Setup screen showing the Secure Nested Paging Coverage setting

IOMMU

This setting must be set to Enabled.

Path: UEFI Settings → System Settings → Processors → Secured Core → IOMMU → Enabled

Description: This setting enables Input-Output Memory Management Unit (IOMMU) support. Enables the Input-Output Memory Management Unit and is required for SEV-SNP enablement. The IOMMU is an AMD EPYC feature that manages and translates memory addresses between devices and system memory.

Figure 9: System Setup screen showing the IOMMU setting

UEFI settings are now configured properly to support Confidential Computing.

Change history

Initial Publication: August 2026

Authors

This paper was produced by the following team of specialists:

Dave Feisthammel is a Senior Solutions Architect working at the Lenovo Center for Microsoft Technologies in Bellevue, Washington. He has over 25 years of experience in the IT field, including four years as an IBM client and 14 years working for IBM. His areas of expertise include Windows Server and systems management, as well as virtualization, storage, and cloud technologies. He is currently a key contributor to Lenovo solutions related to Microsoft Azure Stack Hub, Azure Stack HCI, and Storage Spaces Direct.

Andreina Vivas Thomas is an Advisory Software Engineer working at the Lenovo Center for Microsoft Technologies in Bellevue, Washington. She has worked at Lenovo for over 8 years, specializing in Microsoft on-premises, cloud solutions, developing automation update tools for Azure Stack Hub and Azure Local as well as managing Windows Server enablement and certification as Project Manager.

David Ye is a Principal Solutions Architect at Lenovo with over 25 years of experience in the IT field. He started his career at IBM as a Worldwide Windows Level 3 Support Engineer. In this role, he helped customers solve complex problems and critical issues. He is now working in the Lenovo Infrastructure Solutions Group, where he works with

customers on Proof of Concept designs, solution sizing and reviews, and performance optimization. His areas of expertise are Windows Server, SAN Storage, Virtualization and Cloud, and Microsoft Exchange Server. He is currently leading the effort in Microsoft solutions development, including Azure Local, Foundry Local for Microsoft Sovereign Private Clouds (On-Prem AI Inferencing), Windows Server, and others.

Thanks to the following Lenovo colleagues for their contributions to this project:

- Daniel Ghidali, Manager - Microsoft Technology and Enablement
- Garrett Tashiro, Microsoft Cloud Solution Engineer
- David Watts, Senior IT Consultant - Lenovo Press

At Lenovo Press, we bring together experts to produce technical publications around topics of importance to you, providing information and best practices for using Lenovo products and solutions to solve IT challenges.

See a list of our most recent publications at the Lenovo Press web site:

http://lenovopress.com

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to: Lenovo (United States), Inc. 1009 Think Place - Building One Morrisville, NC 27560 U.S.A.

Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2026. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by Global Services Administration (GSA) ADP Schedule Contract **105**

This document LP2484 was created or updated on August 3, 2026.

Send us your comments via the **Rate & Provide Feedback** form found at http://lenovopress.com/lp2484

Trademarks

Lenovo, the Lenovo logo, and For Those Who Do are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. These and other Lenovo trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by Lenovo at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of Lenovo trademarks is available on the Web at http://www.lenovo.com/legal/copytrade.html.

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo®	Lenovo(logo)®	vNIC™
Lenovo XClarity™	ThinkAgile™	
RackSwitch™	ThinkSystem™	

The following terms are trademarks of other companies:

Intel, Xeon, and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Active Directory, Azure, Hyper-V, Microsoft, PowerShell, SQL Server, Windows, Windows Server, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.